ICOT Technical Report: TR-329

TR-329

# Computing Primitive Elements for Extension Fields

by
K.Yokoyama, M. Noro & T. Takeshima

November, 1987



ICOT
Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan
(03) 456-3191~5
Telex ICOT J32964

Institute for New Generation Computer Technology

# Computing Primitive Elements for Extension Fields

by

Kazuhiro Yokoyama*

Masayuki Noro**

Taku Takeshima***

*Research Associate, Fundamental Informatics Section,

**Research Associate, 1st Collaborate Development Section,

***Senior Research Staff, 1st Collaborate Development Section.

International Institute for Advanced

Study of Social Information Science,

FUJITSU LIMITED

## Abstract

In the problems of Computer Algebra, we often need to treat algebraic extension fields, especially in the problems of polynomial factorization and integration of rational functions.

Several mathematical results and new computational methods are presented for primitive elements and their minimal polynomials.

For a field $Q(\alpha, \beta)$ obtained by adjoining two algebraic numbers $\alpha$ and $\beta$ to the rational number field $Q$, it is shown that there is at least one integer $t$ in distinct $N$ integers such that $\alpha + t\beta$ is a primitive element, where $N$ is the degree of $Q(\alpha, \beta)$ over $Q$. Moreover a method for calculating directly an integer $t$ such that $\alpha + t\beta$ is a primitive element is presented. Finally for given polynomial $F$ over $Q$, methods are presented for computing a primitive element of the splitting field of $F$ and its minimal polynomial over $Q$.

## 1. Introduction

For many applications in Computer Algebra, it becomes more necessary to deal with algebraic numbers. For example, the symbolic integration of rational polynomial requires operating in an extension field obtained as a subfield of the splitting field of its denominator. There are several approaches to describe extension fields in actual problems and applications. Sometimes algebraic numbers should be computed numerically or expressed in terms of radicals. But if we attempt to factor or integrate polynomials symbolically, we have to deal with extension fields in a precise, general and effective way. One promising way is to describe extension fields of the rational field $Q$ as polynomial factor rings. For an extension field $K$ over $Q$ generated by one algebraic number $\alpha$, $K$ is usually described as $Q[x]/ < F(x) >$, where $F(x)$ is the minimal polynomial over $Q$, i.e. a monic irreducible polynomial over $Q$ which has $\alpha$ as a root. But for more complicated extension fields generated by finitely many algebraic numbers, there have been only a few discussions about how to describe them as far as authors know.

In this papar such extension fields are considered. Since an extension field $K$ generated by finitely many algebraic numbers has primitive elements, i.e. $K$ is also generated by only one element, an approach may be used where we find a primitive element $\alpha$ and describe $K$ as $Q(\alpha)$. Here, we employ this approach and discuss methods for finding primitive elements.

Trager (1976), Loos (1982) and Landau (1985) discussed this approach and presented some methods for finding primitive elements. It might be observed that their methods for finding primitive elements, i.e. computing their minimal polynomials, follow essentially from the same idea. That is, they are all based on the results of Kronecker and van der Waerden. ( see van der Waerden(1941). ) They use resultants of polynomials in actual computations. Differences between their methods are in their motivations and applications.

Under the same idea as in their papers, we present some new methods and mathematical basis for computing a primitive element of a field generated by two algebraic numbers, and for the splitting field of a polynomial over $Q$. The remainder of this paper is organized as follows. In Section 2 we discuss necessity to compute primitive elements of finite extension fields. In Section 3 we discuss two methods, namely a trial method and

a deterministic method for finding a primitive element of field generated by two algebraic integers. We present a deterministic method by using bounds of absolute values of algebraic integers. As for a trial method, we present an upper-bound of the number of trials. Moreover in actual computation of the minimal polynomial of a primitive element, we introduce a method using linear equations instead of resultants. In Section 4 we present a deterministic method for finding primitive elements of splitting fields.

## 2. Description of Finite Extension Fields

In dealing with algebraic numbers over $Q$ on computers, it is an important problem how should they be defined on computers. Some are defined in terms of radicals such as $\alpha = 1 + \sqrt{2}$, some are defined as roots of polynomials, and others are defined as rational polynomials in algebraic numbers which have already been defined. Anyway, for Computer Algebra, algebraic numbers are treated as symbols or variables with constraints. Moreover, in order to be able to treat compositions of algebraic numbers which have already been defined, it is necessary that algebraic numbers are treated as variables. So a finite extension field is conveniently described as a polynomial ring over Q with generators as variables. To be exact, an extension field is described as a polynomial factor ring modulo an ideal associated with algebraic relations among algebraic numbers. Such a description would be adopted.

### 2.1. Extension Generated by One Element

We consider an extension field $Q(\alpha)$ generated by an algebraic number $\alpha$. Let $\alpha$ be defined by its minimal polynomial $F_\alpha$. Then there is an isomorphism from $Q(a)$ to $Q[x]/ < F_\alpha(x) >$, where $< F_\alpha >$ is the ideal generated by $F_\alpha$. So we identify $Q(\alpha)$ with $Q[x]/ < F_\alpha(x) >$ as fields. By this identification, the arithmetic, i.e. the operations of addition, subtraction, multiplication and division, can be done on computers as follows. Elements of $Q(\alpha)$ are expressed by polynomials in $\alpha$ with rational coefficients, and the arithmetic is performed as arithmetic in the polynomial ring $Q[x]$ with a reduction modulo $F_\alpha(x)$. We notice that for any algebraic conjugates $\alpha'$ of $\alpha$ over $Q$, i.e. $\alpha'$ is also a root of $F_\alpha$, $Q(\alpha')$ is also isomorphic to $Q[x]/ < F_\alpha(x) >$.

## 2.2. Extension Generated by Two or More Elements

First we consider extension fields generated by two algebraic numbers. Let $\alpha$ and $\beta$ be algebraic numbers and let $Q(\alpha, \beta)$ be the extension field generated by $\alpha$ and $\beta$. According to Section 2.1, $Q(\alpha)$ is identified with $Q[x]/ < F_\alpha(x) >$, where $F_\alpha$ is the minimal polynomial over $Q$. Let $F_\beta$ be the minimal polynomial of $\beta$ over $Q$, and $G_\beta$ over $Q(\alpha)$. Then there is an isomorphism from $Q(\alpha, \beta)$ to $Q[x, y]/ < F_\alpha(x), G_\beta(y; x) >$, where $< F_\alpha(x), G_\beta(y; x) >$ is the ideal generated by $F_\alpha(x)$ and $G_\beta(y; x)$, and $G_\beta(y; x)$ is $G_\beta(y)$ with x's substituted for $\alpha$'s. We notice that $G_\beta$ is not always equal to $F_\beta$. $G_\beta$ is a factor of $F_\beta$ irreducible over $Q(\alpha)$. So if $\beta$ is defined only by $F_\beta$, there is a possibility that $Q(\alpha, \beta)$ can not be determined. In this case, there are candidates for $Q(\alpha, \beta)$ which are obtained by irreducible factors of $F_\beta$ over $Q(\alpha)$. Hence to determine $Q(\alpha, \beta)$, $\beta$ should be defined by $G_\beta$.

The arithmetic on $Q(\alpha, \beta)$ can be performed as arithmetic on a bi-variate polynomial ring with a reduction modulo $< F_\alpha(x), G_\beta(y; x) >$. But this arithmetic is rather complicated, since the Euclidean algorithm can not be applied directly for a reduction modulo $< F_\alpha(x), G_\beta(y; x) >$. So simple arithmetic is needed as in $Q(\alpha)$. It is well-known that a finite extension field $K$ of $Q$ has its primitive element $\gamma$, i.e. $K = Q(\gamma)$. Then if we have the following two algorithms, namely one which computes a primitive element $\gamma$ of $Q(\alpha, \beta)$ and its minimal polynomial over $Q$, and one by which $\alpha$ and $\beta$ can be represented as polynomials in $\gamma$ over $Q$, then the arithmetic on $Q(\alpha, \beta)$ can be more efficiently performed on computers. This is the reason for the necessity of primitive elements.

Next we consider a finite extension field $K$ generated by $n$ algebraic numbers $\alpha_1, ..., \alpha_n$. We can also compute a primitive element of $K$ and its minimal polynomial over $Q$ by applying the above algorithm repeatedly as follows:

Let $K_i = Q(\alpha_1, ..., \alpha_i)$ for $2 < i \leq n$. Then a primitive element $\beta_i$ of $K_i$ is computed by an algorithm for a primitive element of $Q(\beta_{i-1}, \alpha_i)$. By repeating the process for $i = 2, ..., n$, a primitive element of $K$ is obtained as $\beta_n$.

In the next section, we present algorithms for computing primitive elements of extension fields generated by two algebraic numbers.

## 3. Primitive Elements

In this section we consider algebraic extension fields over $Q$ generated by two algebraic numbers, and we discuss some methods to find primitive elements of these fields. For any algebraic number $\alpha$ over $Q$, there is an integer $n$ such that $n\alpha$ is an algebraic integer. From this, we can assume that algebraic numbers to be added are algebraic integers. It is worth mentioning that an algebraic integer satisfies an irreducible polynomial over $Q$ with integral coefficients.

### 3.1. Preliminary Definitions and Notations

Let $\alpha$ and $\beta$ be algebraic integers. Then there is a unique monic irreducible polynomial with integral coefficients, say $F_\alpha(x)$, such that $F_\alpha(\alpha) = 0$. This polynomial is called the minimal polynomial of $\alpha$ over $Q$. Similarly let $F_\beta(x)$ be the minimal polynomial of $\beta$ over $Q$ and let $G_\beta(x;a)$ be the minimal polynomial over $Q(\alpha)$, where $Q(\alpha)$ is the field generated by $\alpha$. As mentioned before, $F_\alpha$ and $G_\beta$ are needed in order to define the algebraic extension field $Q(\alpha,\beta)$ generated by $\alpha$ and $\beta$. If we use $F_\beta$ to define $\beta$, then there is a possibility that $F_\beta$ is not irreducible over $Q(\alpha)$ and so there is no guarantee of the uniqueness in the construction of the extension field. In this case, we need to choose one irreducible factor of $F_\beta$ in $Q(\alpha)$. Therefore, first we assume that, for the definition of $Q(\alpha,\beta)$, $F_\alpha$ and $G_\beta$ are given. ( Later we discuss the case in which $\beta$ is defined by $F_\beta$. ) Then $Q(\alpha,\beta)$ is defined as follows;

$$Q(a,b) \stackrel{\text{def}}{=} Q[x,y]/ < F_\alpha(x), G_\beta(y;x) >,$$

where $G_\beta(y;x)$ is $G_\beta(y)$ with $x$'s substituted in for $\alpha$'s.

Let $n$ be the degree of $F_\alpha(x)$ and let $m$ be the degree of $G_\beta(y;x)$ with respect to $y$. Then the degree $|Q(\alpha) : Q|$ of $Q(\alpha)$ over $Q$ is equal to $n$. Similarly it follows that $|Q(\alpha,\beta) : Q(\alpha)| = m$ and $|Q(\alpha,\beta) : Q| = nm$. Let $N$ be $nm$. Moreover let $M$ be the degree of $F_\beta(y)$.

### 3.2. Norms

To find out primitive elements of $Q(\alpha,\beta)$, the concept of Norms is useful, and is introduced here. Let $k$ be an arbitrary field with characteristic zero and let $d$ be algebraic over $k$. Then there is the minimal polynomial $P(x)$ of $d$ over $k$. The roots $d = d_1$,

$d_2,...,d_s$ of $P$, where $s$=degree $P(x)$, are called the conjugates of $d$ over $k$. Consider the algebraic extension field $k(d)$ generated by $d$, i.e. $k(d)$ obtained by adjoining $d$ to $k$. For any element $e$ in $k(d)$, $e$ can be represented uniquely as a polynomial $e(d)$ in $d$ of degree less than $s = |k(d) : k|$. Then the conjugates of $e$ relative to $k(d)$ over $k$ are defined as $e(d_1), e(d_2), ..., e(d_s)$. A mapping $Norm$ from $k(d)$ to $k$ is defined as follows;

For an element $e$ in $k(d)$, $\mathrm{Norm}_{k(d)/k(e)}$ is the product of all the conjugates of $e$ relative to $k(d)$ over $k$, i.e.

$$\mathrm{Norm}_{k(d)/k}(e) = \prod_{i=1}^{s} e(d_i).$$

It is well-known that $\mathrm{Norm}_{k(d)/k(e)}$ lies in $k$, and if $e$ is an element in $k$, then $\mathrm{Norm}_{k(d)/k(e)} = e^s$.

We can extend the definition of Norm in natural manner to polynomials with coefficients in $K(d)$. For any polynomial $h$ in $x, y, ...$ with coefficients in $k(d)$, $h$ can be expressed as $h(d, x, y, ...)$ which is a polynomial with coefficients in $k$. Then $h(d_i, x, y, ...)$ is the conjugate of $h$ relative to $k(d)$ over $k$. So $\mathrm{Norm}_{k(d)/k(h)}$ is defined as follows;

$$\mathrm{Norm}_{k(d)/k}(h(x, y, ...)) = \prod_{i=1}^{s} h(d_i, x, y, ...).$$

In general, a mapping $Norm$ from a finite extension $E$ of $k$ to $k$ is defined by using embeddings of $E$ into an algebraic closure $\tilde{k}$ of $k$. Let $s_1, ..., s_r$ be all distinct embeddings of $E$ into $\tilde{k}$. Then for an element $e$ in $E$ and $h(x, y, ...)$ in $E[x, y, ...]$, their conjugate are defined as $e^{s_i}$ and $h(x, y, ...)^{s_i}$, where $h(x, y, ...)^{s_i}$ is obtained from $h(x, y, ...)$ by replacing coefficients by their conjugates by the action of $s_i$. From this, Norms are defined as follows;

$$\mathrm{Norm}_{E/k}(e) = \prod_{i=1}^{r} e^{s_i},$$

$$\mathrm{Norm}_{E/k}(h(x, y, ...)) = \prod_{i=1}^{r} h(x, y, ...)^{s_i}.$$

If $E \supset D \supset k$ is a tower of finite extension fields, then $\mathrm{Norm}_{E/k}$=$\mathrm{Norm}_{E/D}$·$\mathrm{Norm}_{D/k}$. So for the case $E = k(d, d')$ and $D = k(d)$, $\mathrm{Norm}_{k(d,d')/k}$ is also defined as $\mathrm{Norm}_{k(d,d')/k(d)}$· $\mathrm{Norm}_{k(d)/d}$. Later we discuss methods for calculations of Norms.

### 3.3. Finding Primitive Elements From $\{\alpha + t\beta | t \in Z\}$ (I)

Now we show how to find out primitive elements of $Q(\alpha, \beta)$ by using the above Norm. By the well-known result, there exist infinitely many primitive elements of $Q(\alpha, \beta)$

in $\{\alpha + t\beta | t \in Q\}$. Therefore we have only to check the question whether $\alpha + t\beta$ is a primitive element or not. First we consider $\mathrm{Norm}_{Q(\alpha,\beta)/Q(\alpha+t\beta)}$. Let $\tilde{Q}$ be an algebraic closure of $Q$. Then there are $N$ distinct embeddings $s_1, ..., s_N$ of $Q(\alpha, \beta)$ into $\tilde{Q}$. For an embedding $s$, $\alpha^s$ and $\beta^s$ are conjugates of $\alpha$ and $\beta$ over $Q$ respectively. If an embedding $s$ fixes $\alpha$ and $\beta$, then $s$ fixes all element of $Q(\alpha, \beta)$ and so $s$ is an identical embedding. From this, the conjugates pairs $(\alpha^{s_i}, \beta^{s_i})$ are all distinct and so there are $N$ distinct pairs. We have the following lemma directly from the results of Trager (1976), Loos (1982) and Landau (1985).

**Lemma 1.** *(1)* $\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ *is a power of an irreducible polynomial in* $Q[x]$.

*(2)* $\alpha + t\beta$ *is a primitive element if and only if* $\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ *is irreducible in* $Q[x]$.

By Lemma 1, whether $\alpha + t\beta$ is a primitive element or not can be tested by examining whether $\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ is square-free or not. So to obtain a primitive element, we have only to find an integer $t$ such that $\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ is irreducible. We show how many distinct integers are needed to find out such $t$. By Landau (1985), it is shown that the number of integers $t$ such that $\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ is not square-free, is not greater than $N(N-1)/2$ and so we need at most $N(N-1)/2 + 1$ integers to get a primitive element. But by using the property of rationals, we show that this number $N(N-1)/2$ can be reduced to $N$. From now on, we write $H_t(x) = \mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ for simplicity.

**Theorem 1.** *There are at most* $N - 1$ *integers* $t$ *such that* $\alpha + t\beta$ *is not a primitive element of* $Q(\alpha, \beta)$.

*Proof.* Assume that $\alpha + t\beta$ is not a primitive element of $Q(\alpha, \beta)$. Then $H_t$ has repeated roots. So there exist distinct embedding $u$ and $v$ in $\{s_1, ..., s_N\}$ such that $\alpha^u + t\beta^u = \alpha^v + t\beta^v$. This implies that $t = (\alpha^u - \alpha^v)/(\beta^v - \beta^u)$. So the number of integers $t$ such that $\alpha + t\beta$ is not a primitive element, is equal to the number of distinct integers $t$ such that $t = (\alpha^{s_i} - \alpha^{s_j})/(\beta^{s_j} - \beta^{s_i})$ for distinct embeddings $s_i$ and $s_j$. Now we consider the Galois closure $K$ of $Q(\alpha, \beta)$ in $\tilde{Q}$ and its Galois group $G$ over $Q$. Then it follows that the distinct images of $(\alpha, \beta)$ by the action of all elements of $G$ coincide with $N$ distinct conjugates pairs of $(\alpha, \beta)$. From this, we can assume that $u$ and $v$ are

elements of $G$. Since $t$ is an integer, $t$ is fixed by all element of $G$. Therefore for any $g$ in $G$, $t^g = t$ implies that $\alpha^{ug} + t\beta^{ug} = \alpha^{vg} + t\beta^{vg}$. Let $S_t$ be a set consisting of distinct ordered pairs $((\alpha^{g_1}, \beta^{g_1}), (\alpha^{g_2}, \beta^{g_2}))$ of distinct conjugate pairs of $(\alpha, \beta)$ such that $\alpha^{g_1} + t\beta^{g_1} = \alpha^{g_2} + t\beta^{g_2}$, where $g_1$ and $g_2$ are elements of $G$. Then $((\alpha^u, \beta^u), (\alpha^v, \beta^v))$ lies in $S$ and so $((\alpha^{ug}, \beta^{ug}), (\alpha^{vg}, \beta^{vg}))$ lies in $S$ for any $g$ in $G$. Since $G$ is a group, there is some $g'$ in $G$ such that $((\alpha, \beta), (\alpha^{g'}, \beta^{g'}))$ lies in $S_t$. So by seeing the action of $G$ on the conjugates pairs of $(\alpha, \beta)$, at least $N$ ordered pairs lie in $S_t$. There are $N(N-1)$ distinct ordered pairs of distinct conjugates pairs of $(\alpha, \beta)$. Hence the number of distinct integers $t$ such that $t = (\alpha^{s_i} - \alpha^{s_j})/(\beta^{s_j} - \beta^{s_i})$ for some distinct embeddings $s_i$ and $s_j$, is at most $N(N-1)/N$. From this we have the conclusion. Q.E.D.

From Theorem 1, we can find out an integer $t$ in a set consisting of $N$ distinct integers. Obviously $t = 0$ does not give a primitive element. So there is some integer which gives a primitive element in the set $\{1, 2, ..., N-1\}$.

Next we discuss further properties of $H_t$. From now on, we treat $t$ as a variable. Then $H_t$ becomes bi-variate polynomial $H(t, x)$. Then $H(t, x)$ is irreducible over $Q$, since $H(s, x)$ is irreducible for some integer $s$. Let $L(t)$ be the discriminant of $H(t, x)$ as a uni-variate polynomial in $x$. Then $L(t)$ has the following properties.

**Theorem 2.** *(1) $L(t)$ has 0 as an $N(m-1)$-ple root.*

*(2) degree $L(t) = N(N - N/M)$.*

*(3) The multiplicity $S$ of an integral root $s$ of $L(t)$ is a multiple of $N$ . Moreover $|Q(a + sb) : Q| = N^2/(N + S)$.*

*Proof.* (1) From the definition of $L(t)$,

$$L(t) = \prod_{1 \le i \ne j \le N} (\alpha^{s_i} + t\beta^{s_i} - \alpha^{s_j} - t\beta^{s_j}) = \prod_{1 \le i \ne j \le N} (t(\beta^{s_i} - \beta^{s_j}) + \alpha^{s_i} - \alpha^{s_j}).$$

Then the number of distinct ordered pairs $(i, j)$ such that $\alpha^{s_i} = \alpha^{s_j}$ is equal to the multiplicity of 0 as a root of $L(t)$. By the fact that $|Q(\alpha, \beta) : Q(\alpha)| = m$, there are $m$ distinct embeddings which fix $\alpha$. This implies that there are $m(m-1)$ distinct ordered pairs $(i, j)$ such that $\alpha = \alpha^{s_i} = \alpha^{s_j}$. We know that there are $n$ distinct conjugates of $\alpha$. So it follows directly that there are $nm(m-1)$ distinct pairs $(i, j)$ such that $\alpha^{s_i} = \alpha^{s_j}$. Hence $L(t)$ has 0 as an $N(m-1)$-ple root.

(2) Similarly, the number of distinct ordered pairs $(i, j)$ such that $\beta^{s_i} = \beta^{s_j}$ is $M(N/M)(N/M-1)$. So we have the following.

$$\text{degree}L(t) = N(N-1) - M(N/M)(N/M-1) = N(N-N/M).$$

(3) Let $s$ be an integral root of $L(t)$ and let $T = |Q(\alpha + s\beta) : Q|$. By Lemma 1 (1), it follows easily that $H(s, x) = (F_{\alpha+s\beta})^{N/T}$, where $F_{\alpha+s\beta}$ is the minimal polynomial of $\alpha + s\beta$ over $Q$. This implies that for any $s_i$, $\alpha^{s_i} + s\beta^{s_i}$ is an $N/T$-ple root of $H(s, x)$, i.e. $N/T$ embeddings transform $\alpha + s\beta$ to the same value, and the number of distinct values of $\alpha^{s_i} + s\beta^{s_i}$'s is $T$. Therefore the number of distinct ordered pairs $(i, j)$ such that $s = (\alpha^{s_i} - \alpha^{s_j})/(\beta^{s_j} - \beta^{s_i})$ is $(N/T)(N/T-1)T = N(N/T-1)$. Since this number is equal to the multiplicity $S$ of $s$ as a root of $L(t)$, we have $S = N(N/T-1)$. From this, we have (3). Q.E.D.

By Theorem 2, we have the following corollary as an improvement of Theorem 1.

**Corollary.** *There are at most $N - N/M - m + 2$ integers $s$ such that $\alpha + s\beta$ is not a primitive element.*

*Proof.* We use the similar argument as in the proof of Theorem 1. By Theorem 2, $S_0$ consists of $N(m-1)$ distinct pairs. Moreover there are $N(N/M-1)$ distinct pairs such that $\beta^u = \beta^v$. So there are at most $(N(N-1) - N(N/M-1) - N(m-1))/N$ non-zero integers $s$ such that $\alpha + s\beta$ is not a primitive element. By including $t = 0$, we obtain the desired result. Q.E.D.

**Remark.** By using Theorem 2, the leading coefficient $lc(L)$ of $L(t)$ can be expressed as follows:

$$lc(L) = D_\beta^{N(N-N/M)/M(M-1)} D_\alpha^{N(m-1)/n(n-1)},$$

where $D_\alpha$ and $D_\beta$ denote the discriminants of $F_\alpha$ and $F_\beta$ respectively.

We can use $L(t)$ for discriminating integers. Whether an integer $t$ gives a primitive element or not can be tested by examining whether $L(t) = 0$ or $L(t) \neq 0$.

Theorem 1 and Theorem 2 say that we can get a primitive element by at most $N$ trials. So it is not necessary to compute $H(t, x)$ as a bi-variate polynomial, and to compute $L(t)$, if we want any primitive element. But if further extensions of fields are needed, the

form of minimal polynomials of primitive elements becomes important. This is because that minimal polynomials with large coefficients are not dealt easily. So there is a case in which minimal polynomials should have simpler form, i.e. they should have rather small coefficients. For this case, $H(t,x)$ and $L(t)$ are useful. For example, let $l(t) = \sum_i |L_i(t)|$, where $L_i(t)$ is the coefficient of $x^i$ in $L(t)$. Then as the best integer, we can choose $t$ such that $l(t)$ is minimal under the constraint that $L(t) \neq 0$.

### 3.4. Finding Primitive Elements From $\{\alpha + t\beta | t \in Z\}$ (II)

We show that we can obtain deterministically an integer $t$ such that $\alpha + t\beta$ is a primitive element. We define the bounds of roots. $\tilde{Q}$ is embedded in the complex number field $C$. For elements in $\tilde{Q}$, absolute values are defined. Let $V_\alpha$ be a rational number which is greater than the absolute values of any conjugates of $\alpha$, and let $W_\beta$ be a rational number whose inverse is not greater than the absolute value of the differences of any two distinct conjugates of $\beta$ in $C$, i.e. $V_\alpha > |\alpha^{s_i}|$ for $i = 1, ..., n$, and $1/W_\beta \leq |\beta^{s_i} - \beta^{s_j}|$ for $\beta^{s_i} \neq \beta^{s_j}$. Then we have the following theorem.

**Theorem 3.** *Let $r$ be an integer such that $r \geq 2V_\alpha W_\beta$. Then $\alpha + r\beta$ is a primitive element of $Q(\alpha, \beta)$.*

*Proof.* Let $\gamma = \alpha + r\beta$. To show that $\gamma$ is a primitive element we have only to prove that the images of $\gamma$ by embeddings $s_i$ are all distinct. So we show that for distinct $i$ and $j$, $\gamma^{s_i} \neq \gamma^{s_j}$. Assume the contrary. Then $\gamma^{s_i} = \gamma^{s_j}$. Since $r$ is fixed by every embeddings, $\alpha^{s_i} + r\beta^{s_i} = \alpha^{s_j} + r\beta^{s_j}$ and so $r(\beta^{s_i} - \beta^{s_j}) = \alpha^{s_j} - \alpha^{s_i}$. If $\beta^{s_i} = \beta^{s_j}$, then $\alpha^{s_i} = \alpha^{s_j}$. This implies that $s_i = s_j$. So we can assume that $\beta^{s_i} \neq \beta^{s_j}$. Then by the definition of $r$, we have the following inequality:

$$2V_\alpha \leq 2V_\alpha W_\beta |\beta^{s_i} - \beta^{s_j}| \leq r|\beta^{s_i} - \beta^{s_j}| = |\alpha^{s_j} - \alpha^{s_i}| < 2V_\alpha.$$

This is a contradiction. Hence $\gamma^{s_i} \neq \gamma^{s_j}$ for any distinct embeddings $s_i$ and $s_j$. From this, we get $Q(\alpha + r\beta) = Q(\alpha, \beta)$. Q.E.D.

**Remark.** We can also prove Theorem 3 by using the fact that the above $r$ is greater than the maximal absolute value of roots of $L(t)$.

As for the bounds $V_\alpha$ and $W_\beta$, we know the following. ( cf. Mignotte (1982).)

For a polynomial $F(x) = \sum_{i=0}^{d} f^0 + f^1 x + ... + f^d x^d$, let $\|F\| = \sum_{i=0}^{d}(f_0^2 + ... + f_d^2)^{1/2}$ and $|F| = max\{|f_0|, ..., |f_d|\}$. Then we have the following.

$$V_\alpha \geq min\{|F_\alpha| + 1, \|F_\alpha\|\},$$

$$W_\beta \geq min\{(2V_\beta)^{M(M-1)/2-1}/|D_\beta|^{1/2}, M^{(M+1)/2}|F_\beta|^{M-1}/3^{1/2}|D_\beta|^{1/2}\},$$

where $D_\beta$ is the discriminant of $F_\beta$, and $V_\beta$ is the bound for the conjugates of $\beta$ defined similarly as $V_\alpha$.

**Remark.** When $\beta$ is given only by $G_\beta(x;a)$, we need $F_\beta$ to calculate the above bound. By using $\mathrm{Norm}_{Q(\alpha)/Q}$, we can obtain $F_\beta$. As another method, we can calculate the upper bounds of $|D_\beta|$ and $V_\beta$ from $G_\beta$ by using the fact that the coefficients of $G_\beta$' are polynomials of $\alpha$.

By Theorem 3, we do not have to seek an integer $s$ which gives a primitive element. But it is possible that the above bounds become too big and so coefficients of the minimal polynomial of primitive element are very large. So tight bounds are needed for actual computations.

### 3.5. Construction of Norms and Minimal Polynomials

We present two methods to compute Norms or minimal polynomials of elements in $Q(\alpha, \beta)$. One uses resultants of polynomials, and the other uses linear equations. Essentially, there is no difference between the two methods in mathematical sense. They eliminate $\alpha$ and $\beta$ from $x - \alpha - t\beta$ by using $F_\alpha$ and $G_\beta$.

The method using resultants is presented in Trager (1976), Loos (1982) and Landau (1985). So we describe this method briefly. It is well-known that, for an arbitrary field $k$ with characteristic zero and an algebraic number $d$ over $k$ whose minimal monic polynomial is $F$, $\mathrm{Norm}_{k(d)/k}(G(x))$ for a polynomial $G(x)$ in $k(d)[x]$ is equal to the resultant of $F(y)$ and $G(x;y)$ in $y$, where $G(x;y)$ is $G(x)$ with $y$'s substituted for $d$'s, i.e. $\mathrm{Norm}_{k(d)/k}(G(x)) = \mathrm{Res}_y(F(y), G(x;y))$. So we have the following.

$$\mathrm{Norm}_{Q(\alpha,\beta)/Q(\alpha)}(x - \alpha - t\beta) = \mathrm{Res}_z(G_\beta(z;\alpha), x - \alpha - tz),$$

$$\begin{aligned}\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta) &= \mathrm{Norm}_{Q(\alpha)/Q}(\mathrm{Norm}_{Q(\alpha,\beta)/Q(\alpha)}(x - \alpha) \\ &= \mathrm{Res}_y(F_\alpha(y), \mathrm{Res}_z(G_\beta(z;y), x - y - tz))\end{aligned}$$

But we know that $G_\beta$ is the minimal irreducible polynomial of $\beta$ over $Q(\alpha)$ and so $\alpha + t\beta$ is a root of $G_\beta((x - \alpha)/t; \alpha)$. By seeing the degree of $G_\beta$, it follows that

$$\mathrm{Norm}_{Q(\alpha,\beta)/Q(\alpha)}(x - \alpha - t\beta) = t^m G_\beta((x - \alpha)/t; \alpha),$$

and

$$H(t,x) = \mathrm{Norm}_{Q(\alpha,\beta)/Q}(x-\alpha-t\beta) = \mathrm{Res}_y(F_\alpha(y), t^m G_\beta((x-y)/t;y)).$$

Moreover for the computation of the discriminant $L(t)$, we use the following resultant;

$$L(t) = (-1)^{N(N-1)/2}\mathrm{Res}_x(H(t,x), \frac{d}{dx}H(t,x)).$$

Now we present a method using linear equations. We determine the minimal linear relation over $Q$ between $1, \gamma, \gamma^2, ...\gamma^N$ for $\gamma = \alpha + t\beta$, where $t$ is an integer. Let the minimal polynomial of $\gamma$ over $Q$ be $F_\gamma = x^k + D_{k-1}x^{k-1} + ... + D_1 x + D_0$. Then there is a linear relation $\gamma^k + D_{k-1}\gamma^{k-1} + ... + D_1\gamma + D_0 = 0$ between $1, \gamma, \gamma^2, ..., \gamma^k$. Conversely from the minimal relation over $Q$ between $1, \gamma, ..., \gamma^N$ we can form the minimal polynomial of $\gamma$ over $Q$. So there is a one to one correspondence between the minimal polynomials and the minimal linear relations. To find the minimal relation, we treat $Q(\alpha,\beta)$ as a vector space over $Q$ with bases $\{\alpha^i\beta^j | 0 \le i \le n-1 \text{ and } 0 \le j \le m-1\}$. Any element in $Q(\alpha,\beta)$ can be represented as a vector by using constraints $F_\alpha(\alpha)$ and $G_\beta(\beta;\alpha)$. So we have the following.

$$\gamma^0 = 1 \rightarrow \bar{\gamma}^0 = (1,0,...,0),$$

$$\gamma^1 = \alpha + t\beta \rightarrow \bar{\gamma}^1 = (0,1,..,0,t,0,...,0),$$

$$\vdots$$

$$\gamma^k = \alpha^k + kt\alpha^{k-1}\beta + ...t^k\beta^k \rightarrow \bar{\gamma}^k = (D_k, 0, 0, ..., D_{k,m-1,n-1}).$$

Let $\mathrm{M}(k,t)$ be a $(k+1)\cdot N$ matrix with the vector $\bar{\gamma}^i$ as the $i$-th row. If the rank of $\mathrm{M}(k,t)$ is not equal to $k+1$, then there is a linear relation between $1, \bar{\gamma}, ..., \bar{\gamma}^k$. So if we want to obtain the minimal polynomial of $\gamma$, then we need to find the first $k$ such that the rank of $\mathrm{M}(k,t)$ is not equal to $k+1$, and solve the equation $\bar{E}\mathrm{M}(k,t) = 0$. For a non-trivial solution $\bar{E} = (E_0, ..., E_k)$, it follows that $E_k \neq 0$ and $\sum_{i=0}^{k}(E_i/E_k)x^i$ is the minimal polynomial of $\gamma$. Similarly, whether $\gamma$ is a primitive element or not, can be tested by examining whether the matrix $\mathrm{M}(N-1,t)$ is regular or not. For simplicity, we write $\mathrm{M}(t)$ instead of $\mathrm{M}(N-1,t)$. Then we have only to find an integer $t$ such that $\mathrm{M}(t)$ is regular. If $\mathrm{M}(t)$ is regular for some $t$, we get the minimal polynomial $F_{\alpha+t\beta}$ by solving the linear equation $\bar{D}\mathrm{M}(t) = -\bar{\gamma}^N$, where $\bar{\gamma}^N$ is a vector corresponding to $\gamma^N$. For the unique

solution $\bar{D} = (D_0, ..., D_N - 1)$, $\sum_{i=0}^{N} D_i x^i$ is the minimal polynomial of $\gamma$ over $Q$, where $D_N = 1$. Similarly, as in Section 3.3, by treating $t$ as a variable, we obtain the following polynomial $M(t)$ which is similar to $L(t)$.

$$M(t) = \text{detM}(t).$$

Since degree $D_{k,i,j(t)} \leq k$, we have degree $M(t) \leq 0 + 1 + ... + N - 1 = N(N-1)/2$. The set of all distinct roots of $M(t)$ coincides with the set of all distinct roots of $L(t)$.

Moreover we can compute $H(t, x)$ in Section 3.3 by using linear equations. We consider a vector space $V$ with bases $\{\alpha^i \beta^j t^k | 0 \leq i \leq n-1, 0 \leq j \leq m-1 \text{ and } 0 \leq k \leq N-1\}$. Let $\gamma(h, k) = \gamma^h t^k$ for $h + k \leq N$, and let $\bar{\gamma}(h, k)$ be the vector in $V$ corresponding to $\gamma(h, k)$. Let M be an $(N+1)(N+2)/2 \times N^2$ matrix with $\bar{\gamma}(h, k)$ as the $(h, k)$-th row, where the order is lexicographic. Then we have the following.

**Lemma 2.** *There is a unique solution $\bar{E}$ such that $\bar{E}$M=0 and the $(N, 0)$-th component $E(N, 0)$ of $\bar{E}$ is 1.*

*Proof.* Let $\bar{E}' = (E(i, j))$ be a vector such that $H(t, x) = \sum_{i+j \leq N} E'(i, j) t^j x^i$ and $E'(N, 0) = 1$. Then it follows that $\bar{E}'$M=0. Assume that there is another solution $\bar{D} = (\bar{D}(i, j))$ with $D(N, 0) = 1$. Let $H'(t, x) = \sum_{i+j \leq N} D(i, j) t^j x^i$. Consider $H'(t, \gamma)$. Since $\bar{D}$ is a solution of $\bar{D}$M=0, $H'(t, \gamma) = 0 \bmod t^{N+1}$. But $\text{degree}_t H'(t, \gamma) \leq N$. This implies that $H'(t, \gamma) = 0$ and so $\bar{D} = \bar{E}$. Q.E.D.

By Lemma 2, $H(t, x)$ can be obtained also by the unique solution of $\bar{E}$M=0 as follows; For the solution $\bar{E} = (E(i, j))$, let $H(t, x) = \sum_{i+j \leq N} E(i, j) t^j x^i$.

Since the method using linear equations does not require to compute the determinants of matrices, it is more efficient than methods using resultants. Moreover if we use this method, then we can compute the representations of elements in $Q(\alpha, \beta)$ as will be shown in the next section.

### 3.6. Representation of $\alpha$ and $\beta$ by a Primitive Element $\gamma$

In this section we present methods to obtain the polynomials $\alpha(x)$ and $\beta(x)$ such that $\alpha(\gamma) = \alpha$ and $\beta(\gamma) = \beta$. We call these polynomials $\alpha(x)$ and $\beta(x)$ the representations of $\alpha$ and $\beta$ by $\gamma$. Similarly to Section 3.5, there are two methods. One is the method using GCD shown by Loos (1982), and the other is the method using linear equations.

First we mention the method using GCD. This method needs the minimal polynomial $F_\beta(x)$ of $\beta$ over $Q$, and the integer $t$ must not be a root of $L^*$, where $L^*$ is obtained similarly as $L(t)$ by using $F_\beta$ instead of $G_\beta$. ( See Section 3.7.) Consider $\mathrm{GCD}(F_\alpha(\gamma - tx), F_\beta(x))$ in $Q(\gamma)[x]$, where $\gamma = \alpha + t\beta$. Then it follows easily that $\mathrm{GCD}(F_\alpha(\gamma - tx), F_\beta(x)) = x - \beta(\gamma)$ from the fact that both of $F_\beta(x)$ and $F_\alpha(\gamma - tx)$ have $\beta$ as a root. As for $\alpha$, we have the representation $\alpha(x)$ by $\alpha(x) = \gamma - t\beta(x)$.

Next we mention the other method which uses linear equations. In the method using linear equations to obtain a primitive element $\gamma = \alpha + t\beta$ and its minimal polynomial $F_\gamma(x)$, we have already gotten the regular matrix $\mathrm{M}(t)$. By using this $\mathrm{M}(t)$, we consider the following linear equation:

$$\bar{A}\mathrm{M}(t) = (0, 1, 0, ..., 0).$$

By the regularity of $\mathrm{M}(t)$, there exists a unique solution $\bar{A} = (A_0, ..., A_{N-1})$. From this solution, we have the representation $\alpha(x) = \sum_{i=0}^{N-1} A_i x^i$ of $\alpha$. As for $\beta$, we have the representation $\beta(x) = (\gamma - \alpha(x))/t$.

An advantage of the latter method is that for any element $\delta$ expressed by a polynomial in $\alpha$ and $\beta$ over $Q$, we can obtain the representation of $\delta$ by $\gamma$ by solving the linear equation associated with $\delta$ without using the representations $\alpha(x)$, $\beta(x)$ and their product.

### 3.7. The Case Where $\beta$ Is Given by $F_\beta$

When we face actual problems which need arithmetics over algebraic extension fields such as $Q(\alpha, \beta)$, all of algebraic numbers added to $Q$ are possibly given rather by their minimal polynomials over $Q$ such as $F_\beta$, than by the minimal polynomials over the extension added by the former numbers such as $G_\beta$. In this case, as mentioned before, if $F_\beta = G_\beta$, then $Q(\alpha, \beta)$ can be determined uniquely, but if not, there is a possibility that there are at least two extension fields which are not isomorphic to each other, i.e there are some candidates for $Q(\alpha, \beta)$. So we present some methods which compute each primitive elements for each candidates. Actually, we need only to replace $G_\beta$ by $F_\beta$ and similar methods are available.

Let $H^*(t, x)$=$\mathrm{Norm}_{Q(\alpha)/Q}(t^M F_\beta((x - \alpha)/t))$ and let $L^*(t)$ be the discriminant of $H^*(t, x)$ as a polynomial in $x$. Then the following holds.

**Lemma 3.** *There is a one to one correspondence between the factors $H_i(t,x)$ of $H^*(t,x)$ in $Q[t,x]$ and the factors $G_i(x)$ of $F_\beta(x)$ in $Q[x]$ by $H_i(t,x)$=$Norm_{Q(\alpha)/Q}(G_i((x-\alpha)/t))$.*

The proof follows from the fact that Norm is multiplicative, i.e. Norm($AB$)=Norm($A$)·Norm($B$). As a corollary, we have the following.

**Corollary.** *Let $\beta$' be a conjugate of $\beta$ over $Q$. Then $|Q(\alpha,\beta') : Q|$=degree$_x H_j(t,x)$ for some $j$.*

By Lemma 3 and its Corollary, for each conjugate $\beta$' of $\beta$ over $Q$, we can obtain each primitive element of $Q(\alpha,\beta')$ by finding each integer $t$ such that each of $H_j(t,x)$'s is irreducible over $Q$. If we choose an integer $t$ such that $L^*(t) \neq 0$, then every $H_j(t,x)$'s are irreducible over $Q$. So we have the following result concerning with the number of integers needed.

**Theorem 4.** *There are at most $nM(M-1)$ integers $t$ such that $L^*(t) = 0$.*

*Proof.* Similarly as in the proof of Theorem 1, a root $s$ of $L^*$ can be expressed as $s = (\alpha_i - \alpha_j)/(\beta_k - \beta_h)$, where $\alpha_i$ and $\alpha_j$ are the conjugates of $\alpha$ over $Q$ for $1 \leq i,j \leq n$ and $\beta_j$ and $\beta_h$ are the conjugates of $\beta$ over $Q$ for $1 \leq k,h \leq M$. It follows that degree $L^*(t) = nM(nM-n)$ by similar arguments as in Theorem 1. Now we consider the case in which the above $s$ is an integer. There are the following two cases;

(1) Some $H_j(s,x)$ is reducible, or

(2) Every $H_j(s,x)$'s are irreducible, but there are two distinct factors $H_j(t,x)$ and $H_i(t,x)$ of $H^*(t,x)$ as bi-variate polynomials over $Q$ such that $H_j(s,x) = H_i(s,x)$.

For the case (1), the multiplicity $S$ of $s$ as a root of $L^*$ is at least $n$·degree$_x H_j(t,x)$ by Theorem 1. So it follows that $S \geq n$.

For the case (2), it can be easily shown that the multiplicity $S$ of $s$ is at least the degree$_x H_j(t,x)$ by looking at $H_j(t,x) = H_i(t,x)$. Since degree$_x H_j(t,x) \geq n$, we have $S \geq n$ for the case 2. Hence for each cases, the multiplicity of $s$ is at least $n$. From this, the number of integral roots of $L^*$ is at most $nM(nM-n)/n = nM(M-1)$. Q.E.D.

We can also use Theorem 3 for this case. The integer $r$ computed by Section 3.4 gives primitive elements $\alpha + r\beta'$ of $Q(\alpha,\beta')$ for every conjugates $\beta$' of $\beta$.

As for actual computations of Norms, we can use both two methods presented in Section 3.6. Moreover we can also obtain a polynomial $M^*(t)$ instead of $M(t)$.

### 3.8. Algorithms

In this section we present some algorithms which embody methods obtained in the previous Sections 3.3, 3.4, 3.5, 3.6, 3.7. As we have seen, there are essentially two ways to get a primitive element in the form $\alpha + t\beta$. One is a trial method, and the other is a deterministic method. Furthermore there are two choices to compute minimal polynomials, namely by using resultants or by using linear equations.

First we present an existing algorithm which is given by Trager(1976), Loos(1982) and Landau(1985).

**Algorithm 1.** ( Trial+Resultant )

Input: $F_\alpha(x)$ an irreducible monic polynomial over $Q$, and $G_\beta(x;y)$ an irreducible monic polynomial over $Q[y]/ < F_\alpha(y) > [x]$.

Output: $F_\gamma$ an irreducible polynomial of a primitive element $\gamma = \alpha + t\beta$.

$t := 1;$
$m :=$degree$_x G_\beta(x;y);$
$g(x;y) := t^m G_\beta((x-z)/t;y) \bmod F_\alpha(y);$
$G(x) :=$Res$_y(F_\alpha(y), g(x;y));$
while GCD$(G(x), \frac{d}{dx}G(x)) \neq 1$ do
  $t := t+1;$
  $g(x;y) := t^m G_\beta((x-y)/t;y) \bmod F_\alpha(y);$
  $G(x) :=$Res$_y(F_\alpha(y), g(x;y))$
$F_\gamma := G(x);$
Return $F_\gamma$

Algorithm 1 computes the minimal polynomial of a primitive element correctly before $t$ exceeds $N-1$ by Theorem 1, or before $t$ exceeds $N - N/M - m + 1$ by Theorem 2. If we use the method of linear equations, then Algorithm 1 is changed to the following.

**Algorithm 2.** ( Trial+Linear Equation )

Input: $F_\alpha(x)$ an irreducible monic polynomial over $Q$, and $G_\beta(x;y)$ an irreducible monic polynomial over $Q[y]/ < F_\alpha(y) > [x]$.

Output: $F_\gamma$ an irreducible polynomial of a primitive element $\gamma = \alpha + t\beta$.

$n$ :=degree$_x F_\alpha(x)$;
$m$ :=degree$_x G_\beta(x;y)$;
$N := nm$;
$t := 1$;
compute the minimal polynomial $G(x)$ of $\gamma = \alpha + t\beta$ by Algorithm 3;
while degree$_x G(x) \neq N$ do
  $t := t + 1$;
  compute the minimal polynomial $G(x)$ of $\gamma = \alpha + t\beta$ by Algorithm 3;
$F_\gamma := G(x)$;
Return $F_\gamma$

**Algorithm 3.** ( The Minimal Polynomial of $\alpha + t\beta$ by Linear Equations )
Input: $F_\alpha(x)$ an irreducible monic polynomial over $Q$, $G_\beta(x;y)$ an irreducible monic polynomial over $Q[y]/ < F_\alpha(y) >$, and $t$ an integer.
Output: $F_\gamma$ the minimal polynomial of $\alpha + t\beta$ over $Q$.

$n$ :=degree$_x F_\alpha(x)$;
$m$ :=degree$_x G_\beta(x;y)$;
$N := nm$;
$D_{0,0,0} := 1$;
$D_{0,i,j} := 0$ for $(i,j) \neq (0,0)$, where $0 \leq i \leq n$ and $0 \leq j \leq m$;
$k := 1$;
while $k < m$ do
  compute $D_{k,i,j}$'s such that $\gamma^k = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} D_{k,i,j}\alpha^i\beta^j \bmod G_\beta(\beta;\alpha), F_\alpha(\alpha)$
$k := m$;
solve the equation $\bar{E}\mathrm{M}(k,t) = 0$;
while $\bar{E} = 0$ do
  $k := k + 1$;
  compute $D_{k,i,j}$'s such that $\gamma^k = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} D_{k,i,j}\alpha^i\beta^j \bmod F_\alpha(\alpha), G_\beta(\beta;\alpha)$;
  solve the equation $\bar{E}\mathrm{M}(k,t) = 0$
$F_\gamma := \sum_{i=0}^{k} D_i x^i$, where $\bar{E} = (E_0, ..., E_k)$ and $D_i = E_i/E_k$;
Return $F_\gamma(x)$

For Algorithm 1 and Algorithm 2, we can use $L(t)$ or $M(t)$ for finding an integer $t$ which gives a primitive element.

Next we present an algorithm which follows from Theorem 3.

**Algorithm 4.** ( Deterministic )

Input: $F_\alpha(x)$ an irreducible monic polynomial over $Q$, and $G_\beta(x;y)$ an irreducible monic polynomial over $Q[y]/ < F_\alpha(y) > [x]$.
Output: $F_\gamma$ an irreducible polynomial of a primitive element $\gamma = \alpha + t\beta$.

$V_\alpha$ :=an upper bound of the absolute values of roots of $F_\alpha$;
$W_\beta$ :=an upper bound of the inverses of difference of any pairs of distinct roots of $F_\alpha$;
$t$ :=an integer greater than $2V_\alpha W_\beta$;
$F_\gamma(x)$ :=$\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$;
Return $F_\gamma(x)$

$\mathrm{Norm}_{Q(\alpha,\beta)/Q}(x - \alpha - t\beta)$ can be computed by $\mathrm{Res}_y(F_\alpha(y), t^m G_\gamma(x;y))$ or the linear equation $\bar{E}\mathrm{M}(r) = -\bar{\gamma}^N$.

When we have a primitive element $\gamma = \alpha + t\beta$, we have the representation of $\alpha$ and $\beta$ by the following.

**Algorithm 5.** ( Representation by Linear Equation )
Input: $F_\alpha(x)$ an irreducible monic polynomial over $Q$, $G_\beta(x;y)$ an irreducible monic polynomial over $Q[y]/ < F_\alpha(y) > [x]$, and an integer $t$ s.t. $\alpha + t\beta$ is a primitive element of $Q(\alpha, \beta)$.
Output: the representation $\alpha(x)$ and $\beta(x)$ of $\alpha$ and $\beta$ by $\gamma$.

$n$ :=$\mathrm{degree}_x F_\alpha(x)$;
$m$ :=$\mathrm{degree}_x G_\beta(x;y)$;
$N := nm$;
$k := 1$;
while $k < N - 1$ do
  compute $D_{k,i,j}$'s such that $\gamma^k = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} D_{k,i,j}\alpha^i\beta^j \bmod G_\beta(\beta;\alpha), F_\alpha(\alpha)$
solve the equation $\bar{E}M(t) = (0, 1, 0, ..., 0)$;
$\alpha(x) := \sum_{i=0}^{N-1} E_i x^i$, where $\bar{E} = (E_0, ..., E_{N-1})$;
$\beta(x) := (x - \alpha(x))/t$;
Return $\alpha(x)$ and $\beta(x)$

We notice that if we use Algorithm 2 to find an integer $t$, then $D_{k,i,j}$'s are already computed in this process, and so for Algorithm 5 we need not compute $D_{k,i,j}$ again. Finally we present an algorithm for the case where $\beta$ is given only by $F_\beta$. The following algorithm uses $L^*(t)$ for finding an integer $s$.

**Algorithm 6.** ( $\beta$ Is Given by $F_\beta$ )
Input: $F_\alpha$ an irreducible monic polynomial over $Q$, and $F_\beta$ an irreducible monic polynomial over $Q$.

Output: monic irreducible polynomials $F_i$ s.t. $F_i$ is the minimal polynomial of $\gamma_i$ over $Q$, where $Q(\gamma_i) = Q(\alpha', \beta')$ for conjugates $\alpha$' and $\beta$' of $\alpha$ and $\beta$.

$n$ :=degree$_x F_\alpha(x)$;
$M$ :=degree$_x F_\beta(x)$;
$g(t, x; y) := t^M F_\beta((x - y)/t)$;
$H(t, x)$ :=Norm$_{Q(\alpha)/Q}(g(t, x; \alpha))$;
$L(t)$ :=Discriminant$_x(H(t, x))$;
find an integer $s$ s.t. $L(s) = 0$;
factorize $H(s, x)$ to irreducible factors $F_i(x)$ over $Q$;
Return $F_i(x)$

## 4. Splitting Fields of Polynomials

For a polynomial $F(x)$ over $Q$, the splitting field $K$ is obtained by adjoining all roots of $F$ to $Q$. We show some methods to find a primitive element of the splitting field of a polynomial $F$ over $Q$. Methods shown here follow essentially from Theorem 3, and so they need not trial for finding an integer which gives a primitive element. Of course, there are some methods with trial. ( cf. Trager (1976), Landau (1985). ) Moreover it is noted that methods shown here are not repetitve applications of the algorithms in the previous section. For simplicity, let $F(x)$ be a monic irreducible polynomial over $Q$. This can be assumed, since the splitting field of a polynomial is the composite field obtained from all the splitting fields of its factors.

### 4.1. Extension of Theorem 3

Let the roots of $F$ be $\alpha_1, ..., \alpha_n$, where $n$=degree$_x F(x)$, and let $K$ be the splitting field, i.e. $K = Q(\alpha_1, .., \alpha_n)$. Since $\alpha_1 + \cdots + \alpha_n \in Q$, $K$ is generated by $n - 1$ distinct roots of $F$.

We define bounds $V$ and $W$ as in Section 3.4, i.e. $V > |\alpha_i|$ for $i = 1, ..., n$ and $W \geq 1/|\alpha_i - \alpha_j|$ for $i \neq j$. Moreover let $r$ be an integer such that $r \geq 4VW$ and $r \geq 2$. Then we have the following theorem as an extension of Theorem 3.

**Theorem 5.** *Let $\beta_1, ..., \beta_i$ be $i$ distinct roots of $F$ and $\gamma = \beta_1 + r\beta_2 + ... + r^{i-1}\beta_i$. Then $\gamma$ is a primitive element of the extension field $Q(\beta_1, \beta_2, ..., \beta_i)$.*

*Proof.* We prove Theorem 5 by induction. From Theorem 3, we can assume that $i > 2$. Assume that Theorem 5 is true for $i = k$, and consider the case $i = k + 1$. Similarly

to the proof of Theorem 3, to prove $Q(\gamma) = Q(\beta_1, ..., \beta_{k+1})$, we have only to show that $\gamma^{s_j} \neq \gamma^{s_h}$ for any two distinct embeddings $s_j$ and $s_h$ of $Q(\beta_1, ..., \beta_{k+1})$ into $Q$. So assume the contrary, i.e. $\gamma^{s_j} = \gamma^{s_h}$ for some $j \neq h$. Then by the definition of $\gamma$, it follows that $r^k(\beta_{k+1}^{s_j} - \beta_{k+1}^{s_h}) = (\beta_1^{s_h} - \beta_1^{s_j}) + r(\beta_2^{s_h} - \beta_2^{s_j}) + ... + r^{k-1}(\beta_k^{s_h} - \beta_k^{s_j})$. If $\beta_{k+1}^{s_j} = \beta_{k+1}^{s_h}$, then $(\beta_1 + ... + r^{k-1}\beta_k)^{s_j} = (\beta_1 + ... + r^{k-1}\beta_k)^{s_h}$. By the assumption of the induction, $\beta_1 + ... + r^{k-1}\beta_k$ is a primitive element of $Q(\beta_1, ..., \beta_k)$. So $s_j$ and $s_h$ can be considered as embeddings of $Q(\beta_1, ..., \beta_k)$ into $Q$. Then by the assumption of the induction, it follows that $\beta_m^{s_j} = \beta_m^{s_h}$ for $m = 1, .., k$. From this, we get $s_j = s_h$ and this is a contradiction. Therefore we can assume that $\beta_{k+1}^{s_j} \neq \beta_{k+1}^{s_h}$. Consider the absolute values of both sides of the above equation. Then the left-hand side is bounded as follows;

$$\begin{aligned} r^k|\beta_{k+1}^{s_j} - \beta_{k+1}^{s_h}| &= 4VWr^{k-1}|\beta_{k+1}^{s_j} - \beta_{k+1}^{s_h}| \\ &\geq 4Vr^{k-1}. \end{aligned}$$

The right-hand side is bounded as follows;

$$\begin{aligned} |(\beta_1^{s_h} - \beta_1^{s_j}) + ... + r^{k-1}(\beta_k^{s_h} - \beta_k s_j)| &\leq |\beta_1^{s_h} - \beta_1^{s_j}| + ... + r^{k-1}|\beta_k^{s_h} - \beta_k s_j| \\ &< 2V(1 + r + ... + r^{k-1}). \end{aligned}$$

So we have the following inequality.

$$2V(1 + r + ... + r^{k-1}) > 4Vr^{k-1}.$$

This implies that

$$1 + r + ...r^{k-2} > r^{k-1}.$$

But by $r \geq 2$,

$$\begin{aligned} 1 + r + ... + r^{k-2} &= (r^{k-1} - 1)/(r - 1) \\ &< r^{k-1} \end{aligned}$$

Hence this is a contradiction. Q.E.D.

From Theorem 5, we have the following.

**Corollary.** *Let $S = \{\alpha_1, ..., \alpha_n\}$ and $T = \{\beta_1 + r\beta_2 + ... + r^{n-2}\beta_{n-1} | \beta_i \in S\}$. Then there is a primitive element of $K$ in $T$. If $\beta_i$'s are all distinct, then $\beta_1 + ... + r^{n-2}\beta_{n-1}$ is a primitive element of $K$.*

### 4.2. Finding Primitive Elements of Splitting Fields

By using results obtained in Section 4.1, we have the following method to find a primitive element of the splitting field $K$.

Now we define polynomials $g_{(i)}$ by the following.

$g_{(0)} = x$, $g_{(1)} = F(x)$, and for $i \geq 2$ $g_{(i)}$'s are defined by

$g_{(i)} = \mathrm{Norm}_{Q(\alpha)/Q}(g_{(i-1)}(x - r^{i-1}\alpha))$, where $\alpha$ is an arbitrary root of $F$ and $r$ is an integer defined in Theorem 5.

We notice that for the actual computation of $\mathrm{Norm}_{Q(\alpha)/Q}$ we can use either a method using resultants or a method using linear equations. Then $g(i)$ has the following property.

**Theorem 6.** *Each irreducible factor of $g_{(i)}$ over $Q$ is the minimal polynomial of some $\beta_1 + ... + r^{i-1}\beta_i$ over $Q$, where $\beta_1, ..., \beta_i$ are the roots of $F$. Moreover a factor of $g_{(i)}$ with the maximal degree is the minimal polynomial of a primitive element of an extension field with the maximal degree in the extension fields obtained by adjoining $i$ roots of $F$.*

*Proof.* By the definition, it follows that $g_{(i)} = \prod_{\beta_1,...,\beta_i \in S}(x - \beta_1 - r\beta_2 - ... - r^{i-1}\beta_i)$. So $g_{(i)}$ is the composition of all minimal polynomials of $\beta_1 + ... + r^{i-1}\beta_i$'s over $Q$. And degree of $Q(\beta_1 + ... + r^{i-1}\beta_i)$ over $Q$ is equal to degree of the minimal polynomial of $\beta_1 + ... + r^{i-1}\beta_i$. By Theorem 5, $\beta_1 + ... + r^{i-1}\beta_i$ is a primitive element of $Q(\beta_1, .... \beta_i)$. Hence for an extension fields whose degree over $Q$ is maximal in extension fields obtained by adjoining $i$ roots of $F$, the minimal polynomial of a primitive element is a factor of $g_{(i)}$ with the maximal degree. Q.E.D.

As the corollary, we have the following.

**Corollary.** *A factor of $g_{(n-1)}$ with the maximal degree is the minimal polynomial of a primitive element of $K$.*

From this corollary, we can obtain the minimal polynomial of a primitive element of $K$ by factoring $g_{(n-1)}$. But the degree of $g_{(n-1)}$ is $n^{n-1}$ and this implies that actual computations of $g_{(n-1)}$ are almost impossible for computers. So we use factors of $g_{(i)}$.

Let $g_i$ be an irreducible factor of $g_{(i)}$ over $Q$ with the maximal degree and $n_i$ be its degree. $n_i$ is determined independently of the choice of $g_i$. Then we have the following.

**Theorem 7.** *For $1 \leq i < n$, $n_i \leq n_{i+1}$. If $n_1 < n_2 < ... < n_{k-1}$ and $n_{k-1} = n_k$ for some $k < n$, then $g_{k-1}$ is the minimal polynomial of a primitive element of $K$. If $n_1 < ... < n_{n-1}$, then $g_{n-1}$ is the minimal polynomial of a primitive element of $K$.*

*Proof.* By the definition, it can be easily seen that $g_i$ is the minimal polynomial

of $\beta_1 + r\beta_2 + ... + r^{i-1}\beta_i$, where $\beta_1, ..., \beta_i$ are the roots of $F$. By Theorem 5, we have $n_i = |Q(\beta_1, ..., \beta_i) : Q|$. As for $g_{(i+1)}$, $g_{(i+1)}$ is the product of all minimal polynomials of elements $\gamma_1 + ... + r^i\gamma_{i+1}$, where $\gamma_j$' are roots of $F$. So $g_{(i+1)}$ has the minimal polynomial of $\beta_1 + ... + r^{i-1}\beta_i + r^i\beta_{i+1}$ as a factor, where $\beta_{i+1}$ is a root of $F$. By the definition, it follows that $n_{i+1} \geq |Q(\beta_1, ..., \beta_{i+1}) : Q|$. Since $|Q(\beta_1, ..., \beta_{i+1}) : Q(\beta_1, ..., \beta_i)| \geq 1$, we have $n_i \leq n_{i+1}$.

Next consider the case $n_1 < ... < n_{k-1}$ and $n_{k-1} = n_k$ for $k < n$. Let $\beta_1, ..., \beta_{k-1}$ be roots of $F$ such that $g_{k-1}$ is the minimal polynomial of $\beta_1 + ... + r^{k-2}\beta_{k-1}$. If $Q(\beta_1, ..., \beta_{k-1})$ is not the splitting field $K$, then there is some root $\beta_k$ which does not belong to $Q(\beta_1, ..., \beta_{k-1})$. This implies that $|Q(\beta_1, ..., \beta_{k-1}, \beta_k) : Q(\beta_1, ..., \beta_{k-1})| > 1$ and so the degree of the minimal polynomial of $\beta_1 + ... + r^{k-1}\beta_k$ over $Q$ is greater than $n_{k-1}$. From the definition of $g_{(k)}$, $g_{(k)}$ has the minimal polynomial of $\beta_1 + ... + r^{k-2}\beta_{k-1} + r^{k-1}\beta_k$ as its factor. This implies that $n_{k-1} < n_k$ and a contradiction. Hence for this case, $g_{k-1}$ is the minimal polynomial of a primitive element of $K$. If $n_1 < ... < n_{n-1}$, then $g_{n-1}$ is the minimal polynomial of $\beta_1 + ... + r^{n-2}\beta_{n-1}$. By the previous argument, it can be easily shown that $\beta_i$'s are all distinct. Hence by Corollary of Theorem 5, $\beta_1 + ... + r^{n-2}\beta_{n-1}$ is a primitive element of $K$ and so $g_{n-1}$ is the minimal polynomial of a primitive element of $K$. Q.E.D.

By the above theorem, an algorithm using $g_i$'s terminates when $n_k = n_{k+1}$ or $k = n$. But there are many unnecessary factors in $g_{(k)}$'s. So we have the following improvement.

Instead of $g_i$, we construct polynomials $h_{(i)}$ and $h_i$ inductively by the following;

$h_{(1)} = h_1 = g_{(1)} = F$, and if $h_{i-1}$ is already constructed, then

$h_{(i)}$=Norm$_{Q(\alpha)/Q}(h_{i-1}(x - r^{i-1}\alpha)$ and $h_i$ is an irreducible factor of $h_{(i)}$ with the maximal degree over $Q$, where $\alpha$ is an arbitrary root of $F$.

Let $N_i$ =degree $h_i$. By replacing $g_{(i)}$ and $g_i$ by $h_{(i)}$ and $h_i$ in the argument of the proof of Theorem 7, we have the following Theorem.

**Theorem 8.** *For $1 \leq i < n$, $N_i \leq N_{i+1}$. If $N_1 < N_2 < ... < N_{k-1}$ and $N_{k-1} = N_k$ for some $k < n$, then $h_{k-1}$ is the minimal polynomial of a primitive element of $K$. If $N_1 < ... < N_{n-1}$, then $h_{n-1}$ is the minimal polynomial of a primitive element of $K$ and this implies that to obtain $K$ it needs all the roots of $F$.*



603

Now, we discuss the algorithms. There may be several ways in actual computations. Among them we show two algorithms,one as a basic version, and the other improved one. The basic version is a naive algorithm based on the Corollary of Theorem 6, and is shown as Algorithm 7. It can be easily understood and helps understanding the rather complicated improved version. Notice that this algorithm itself is almost impractical because it always requires factoring $g_{(n-1)}$ a vast polynomial with degree $n^{n-1}$, even when the degree of extension is much less than $n^{n-1}$.

On the other hand, the improved version shown as Algorithm 8 is based on Theorem 8, and is more practical. Since it repeatedly constructs intermediate extension fields by adjoining roots of the given polynomial, swell of the degree of intermediate polynomial $h_i$ can be limited, if we design the algorithm carefully, to $n \cdot N_{i-1}$ at $i-$th repetition, where $h_i$ and $N_{i-1}$ are given in Theorem 8. Although, in the worst case, $N_i$ increases to $n!$ as $i$ reaches $n$, it is obviously practical to construct extension fields successively, when the degree of the splitting field is relatively small.

New method presented in Algorithm 8 has an advantage over other methods as was presented by Trager (1976) and Landau (1985). It requires neither trial seeking for integers nor making choice on which root should be adjoined.

Since in the new method, a primitive element is determined first, the algorithm need not toil for factoring $F$ over extension fields, but for factoring $h_{(i)}$, over $Q$, which are obtained by calculations over $Q[x]/ < F(x) >$. So except for the growth of coefficients of minimal polynomials, new method is more efficient than methods already proposed.

By using $h_k$, we can also compute the minimal polynomial of a primitive element of $K$.

**Remark.** There is the following correspondence between irreducible factors of $g_{(m)}$ over $Q$ and sets consisting of ordered $m$-tuple of roots of $F$.

Let $S$ be the set consisting of all roots of $F$, i.e. $S = \{\alpha_1, ..., \alpha_n\}$, and $T_m$ be the set consisting of all ordered $m$-tuple of roots of $F$, i.e. $T_m = S \cdot S \cdots S = S^m$. The action of $G$ on $T_m$ is defined naturally by $(\beta_1, ..., \beta_m)^g = (\beta_1^g, ..., \beta_m^g)$ for $(\beta_1, ..., \beta_m) \in T_m$ and $g \in G$. For a subset $B$ in $T_m$, $B$ is said to be $G$-invariant if $B^g = B$ for any $g$ in $G$. Then there is a one to one correspondence between irreducible factors of $g_{(m)}$ over $Q$ and minimal $G$-invariant subsets of $T_m$. The correspondence is described by the following.

Let $B$ be a minimal $G$-invariant subset of $T_m$. We define a polynomial $h_B$ by $h_B = \prod_{\bar{b} \in B}(x - \beta_1 - r\beta_2 - ... - r^{m-1}\beta_m)$, where $\bar{\beta} = (\beta_1, ..., \beta_m)$. Then it can be shown that $h_B$ is a polynomial over $Q$ by the $G$-invariance of $B$. Moreover the minimality of $B$ implies that $h_B$ can not be factored over $Q$, i.e. $h_B$ is irreducible over $Q$. Conversely for an irreducible factor $h$, let $B_h$ be the subset consisting of all $\bar{b}$ such that $\bar{b} = (\beta_1, ..., \beta_m)$ and $\beta_1 + ... + r^{m-1}\beta_m$ is a root of $h$. Then the fact that $h$ is a polynomial over $Q$ implies that $B_h$ is $G$-invariant, and the irreducibility of $h$ implies the minimality of $B_h$. Hence an irreducible factor $h$ over $Q$ corresponds to a minimal $G$-invariant subset $B_h$.

For any minimal $G$-invariant subset $B$, the cardinality $|B|$ is equal to the index of the stabilizer $G_{\bar{b}}$ of $G$ in $G$ for an element of $\bar{b}$ of $B$, i.e. $|B| = |G : G_{\bar{b}}|$, where the stabilizer $G_{\bar{b}} = \{g \in G | \bar{b}^g = \bar{b}\}$. Since degree $h_B = |B|$ by the previous correspondence, it follows that degree $h_B = |G : G_{\bar{b}}|$. From this, $h_B$ is the minimal polynomial of a primitive element of $K$ if and only if $G_{\bar{b}} = 1$ for $\bar{b}$ in $B$. Especially if $m = n - 1$ and components of $\bar{b}$ are all distinct, then $G_{\bar{b}} = 1$ and $h_B$ is the minimal polynomial of a primitive element of $K$.

### 4.3. Algorithms and Remarks

It seems very difficult to compute minimal polynomials of primitive elements of splitting fields by existing computers. This is because, in the worst case, the degree of the splitting field is $n!$, where $n$ is the degree of a given polynomial to be split. But if $n$ is small or the degree of the splitting field is much less than $n!$, there is a possibility that the minimal polynomial of a primitive element can be computed.

**Algorithm 7. ( The basic algorithm )**

Input: $F$ an irreducible polynomial over $Q$.

Output: $G$ the minimal polynomial of a primitive element of the splitting field.

$n$ :=degree $F$;
$V$ :=an upper bound of the absolute values of roots of $F$;
$W$ :=an upper bound of the absolute values of inverses
  of differences of any two distinct roots of $F$;
$r$ :=an integer greater than $4VW$;
$i := 1$;
$g_{(1)} := F(x)$;
while $i \leq n$ do
  $g_{(i)}$ :=$\mathrm{Norm}_{Q(\alpha)/Q}(g_{(i-1)}(x - r^{i-1}\alpha))$, where $\alpha$ is an arbitrary root of $F$;
factorize $g_{(n)}$ to irreducible factors in $Q$;
$G$ :=an irreducible factors of $g_{(i)}$ with the maximal degree;
Return $G$

**Algorithm 8. ( The improved algorithm )**

Input: $F$ an irreducible polynomial over $Q$.

Output: $G$ the minimal polynomial of a primitive element of the splitting field.

$n$ :=degree $F$;
$V$ :=an upper bound of the absolute values of roots of $F$;
$W$ :=an upper bound of the absolute values of inverses of
  differences of any two distinct roots of $F$;
$r$ :=an integer greater than $4VW$;
$N_0 := 1$;
$i := 1$;
$h_1 := F(x)$;
$N_1 := n$;
while $N_i \neq N_{i-1}$ do
  $i := i + 1$;
  $h_{(i)}$ :=$\mathrm{Norm}_{Q(\alpha)/Q}(h_{i-1}(x - r^{i-1}\alpha))$, where $\alpha$ is an arbitrary root of $F$;
  factorize $h_{(i)}$ to irreducible factors in $Q$;
  $h_i$ :=an irreducible factors of $h_{(i)}$ with the maximal degree;
  $N_i$ :=degree $h_i$;
$G := h_{i-1}$;
Return $G$

**Acknowledgements**

The authors would like to acknowledge the continuing encouragement of Dr. T. Kitagawa, the president of their institute, and Dr. H. Enomoto, the director of their institute. They also thank Dr. H. Kano for his comments on the draft of this paper.

This is part of the work in the major R&D of the Fifth Generation Computer Project, conducted under program set up by MITI.

## References

von zur Gathen, J. (1984). Pallarel algorithms for algebraic problems. SIAM J. Compt. **13**. 802-824.

Landau, S. (1985). Factoring polynomials over algebraic number fields. SIAM J. Compt. **14**. 184-195.

Lang, S. (1976). Algebra. 8th ed. Reading, Massachusetts. Addison-Wesley

Lenstra, A. K. (1983). Factoring polynomials over algebraic number fields Computer Algebra. Springer Lec. Note Comp. Sci. **162**. 245-254.

Loos, R. (1982). Computing in algebraic extensions. In: ( Buchberger, B. et al., eds ) Computer Algebra ( Computing Supplement **4** ). 173-187. New York. Springer-Verlag.

Mignotte, M. (1982). Some useful bounds. In: ( Buchberger, B. et al., eds ) Computer Algebra ( Computing Supplement 4 ). 259-263. New York. Springer-Verlag.

Trager, B. M. (1976). Algebraic factoring and rational integration. Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation.

van der Waerden, B. L. (1971). Algebra I. Berlin-Heidelberg-New York. Springer.

Weinberger, P. J., Rothschild, L. P. (1976). Factoring polynomials over algebraic number fields. ACM Transaction on Mathematical Software **2**. 335-350.