J. Symbolic Computation (1996) **11**, 1–000

On Computing Subfields

JÜRGEN KLÜNERS AND MICHAEL POHST

Technische Universität Berlin, Fachbereich 3, Sekr. MA 8-1,

Straße des 17. Juni 136, 10623 Berlin, Germany

E-mail address: klueners, pohst@math.tu-berlin.de

(Received 7 September 1996)

The purpose of this article is to determine all subfields $\mathbb{Q}(\beta)$ of fixed degree of a given algebraic number field $\mathbb{Q}(\alpha)$. It is convenient to describe each subfield by a pair (h,g) of polynomials in $\mathbb{Q}[t]$ resp. $\mathbb{Z}[t]$ such that g is the minimal polynomial of $\beta = h(\alpha)$. The computations are done in unramified p-adic extensions and use information concerning subgroups of the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ obtained from the van der Waerden criterion.

1. Introduction

Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field of degree n which is given by a zero α of the corresponding minimal polynomial $f \in \mathbb{Z}[t]$. In this article a method for determining all subfields $L = \mathbb{Q}(\beta)$ of K of fixed degree m over $\mathbb{Q}$ is developed. We describe each subfield L by the minimal polynomial g of β and and the embedding of β into K, which is given by a polynomial $h \in \mathbb{Q}[t]$ with $h(\alpha) = \beta$.

LEMMA 1.1. *1 Each subfield L of K has a representation by a pair (h,g) with $g(h) \equiv 0 \bmod f\mathbb{Z}[t]$.*
2 A pair (h,g) with $g(h) \equiv 0 \bmod f\mathbb{Z}[t]$ describes a subfield L of K.

Note that the coefficients of the *embedding polynomial* h are not necessarily integral because the equation order $\mathbb{Z}[\alpha]$ is in general not a maximal order. W.l.o.g. we assume that the degree of h is smaller than n, because h can be replaced by its remainder modulo f. The lemma is used to check if a pair (h,g) presents a subfield L of K. Such a subfield L is represented in the form $\mathbb{Q}[t]/g(t)\mathbb{Q}[t]$; hence isomorphic fields are not distinguishable.

EXAMPLE 1.2. *We determine all subfields L of $K = \mathbb{Q}(i\sqrt[6]{108})$ of degree 3. There are three subfields with characterizing pairs $(-t^2, t^3-108)$, $(\frac{1}{12}t^5 + \frac{1}{2}t^2, t^3-108)$ and $(-\frac{1}{12}t^5 + \frac{1}{2}t^2, t^3-108)$. In all cases the minimal polynomial of β is the same; however, we are able to distinguish the generated subfields by their embedding polynomials.*

There are at least six other algorithms [Casperson, Ford, McKay (1995), Cohen, Diaz y Diaz (1991), Dixon (1990), Hulpke (1995), Landau, Miller (1985), Lazard, Valibouze

0747–7171/90/000000 + 00 $03.00/0

(1993)] for calculating subfields. In this article we generalize and improve the methods of Dixon (1990). The generating polynomials are constructed by factorizations over finite fields and Hensel lifting over p-adic fields. Three other methods [Hulpke (1995), Landau, Miller (1985), Lazard, Valibouze (1993)] need factorizations of polynomials over number fields, respectively factorizations of polynomials over the rational integers of much higher degree than the degree of the given field. These factorizations are very expensive. The method presented in Casperson, Ford, McKay (1995) needs hard numerical computations and lattice reduction algorithms. Finally, the algorithm in Cohen, Diaz y Diaz (1991) computes subfields, too. But it is not guaranteed that all subfields will be found. A comparison of running times is given in section 6.

2. Blocks of Imprimitivity and the Relation to Subfields

Let $G = \mathrm{Gal}(f)$ be the Galois group of a splitting field N of f and $\Omega = \{\alpha = \alpha_1, \dots, \alpha_n\}$ be the set of zeros of f in N. Considered as a permutation group of the set of roots, G operates transitively on Ω because f is irreducible.

DEFINITION 2.1. *1 $\emptyset \neq \Delta \subseteq \Omega$ is called a* **block of imprimitivity** *(block), if $\Delta^\tau \cap \Delta \in \{\emptyset, \Delta\}$ for all $\tau \in G$.*

2 $\Delta = \{\alpha_i\}$ $(1 \leq i \leq n)$ and $\Delta = \Omega$ are called **trivial blocks**. *G is called* **imprimitive** *if there exists a non-trivial block. Otherwise G is called* **primitive**.

3 Blocks $\Delta_1, \dots, \Delta_m$ with $\Delta_i \neq \Delta_j$ $(1 \leq i < j \leq m)$ are called a (complete) **block system**, *if the set $\{\Delta_1, \dots, \Delta_m\}$ remains invariant under G.*

If Δ is a block, it is easy to see that Δ^τ $(\tau \in G)$ is also a block. Note that each block lies in exactly one complete block system $\Delta_1, \dots, \Delta_m$ with $\Delta_i = \Delta^{\tau_i}$ for a suitable element $\tau_i \in G$.

The connection between blocks and subfields is based on the following two theorems.

THEOREM 2.2. *(Fundamental Theorem of Galois Theory)*
Let $M = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ be the splitting field of f and $G = \mathrm{Gal}(M/\mathbb{Q})$.

1 Every intermediate field $\mathbb{Q} \subseteq L = \mathbb{Q}(\beta) \subseteq M$ corresponds to a subgroup H of G and vice versa.

2 L is a Galois extension if and only if H is a normal subgroup of G.

3 The subfields L of K correspond to the groups $H \subseteq G$ containing G_α, the fix group of α.

THEOREM 2.3. *The lattice of groups between G_α and G is isomorphic to the lattice of blocks of G which contain α.*

The proof of theorem 2.3 can be found in Wielandt (1964).

REMARK 2.4. *Let L_1 and L_2 be two subfields of K with corresponding blocks B_1 and B_2 containing α. Then $B = B_1 \cap B_2$ is a block which contains α as well. It corresponds to a subfield $L = L_1 L_2$ of K. Furthermore L_1 is a subfield of L_2 if and only if $B_1 \supseteq B_2$.*

As each block is part of a complete block system, by the preceding theorems there is a connection between complete block systems and subfields. Let $\Delta_1, \ldots, \Delta_m$ be a complete block system, $H = G_{\Delta_1}$ and L be the subfield fixed by H. Define

$$\delta_i := \prod_{\gamma \in \Delta_i} \gamma \quad (i = 1, \ldots, m).$$

It is easy to see that $\delta_1 \in L$ and $\delta_i \, (i = 2, \ldots, m)$ are conjugates of δ_1. The polynomial

$$g(t) := \prod_{i=1}^{m} (t - \delta_i)$$

is the characteristic polynomial of δ_1 in L and is of the form: $g(t) = \tilde{g}(t)^j$ ($j \in \mathbb{N}$, $\tilde{g} \in \mathbb{Z}[t]$ monic and irreducible). Now there are two possibilities. In the first case the polynomial g is irreducible, hence generates the subfield L. In the other case the δ_i are not pairwise distinct, requiring that we search for another generating polynomial of K such that the δ_i become distinct. To do this, $f(t)$ is replaced by $f(t-k)$ ($k \in \mathbb{Z}$). In Dixon (1990) it is proved that at most $\frac{1}{2}mn$ substitutions of this type do not yield irreducible polynomials.

The problem of calculating a generating polynomial of the subfield L is reduced to the determination of the corresponding block system $\Delta_1, \ldots, \Delta_m$. Of course, this reduction is purely theoretical so far, since neither the Galois group G nor its operation on Δ are known.

For practical applications Dixon (1990) suggested to make use of van der Waerden's criterion (1971).

Theorem 2.5. *(van der Waerden's Criterion)*
Let R be a UFD, $\mathfrak{p}$ a prime ideal in R, $\bar{R} := R/\mathfrak{p}$ its residue class ring, $f \in R[t]$ and $\bar{f} \in \bar{R}[t]$ with $f \equiv \bar{f} \bmod \mathfrak{p}$. If $\bar{f}$ is square-free, it follows that $\bar{G} = \mathrm{Gal}(\bar{f})$ is isomorphic to a subgroup of $G = \mathrm{Gal}(f)$.

The van der Waerden criterion allows us to determine cyclic subgroups of G which are generated by a permutation $\pi \in G$. Let $\pi = \pi_1 \cdots \pi_u$ be the decomposition of π into disjoint cycles and $n_i = |\pi_i|$ the number of zeros permuted by π_i ($1 \le i \le u$). We say that π is of **cycle type** $[n_1, \ldots, n_u]$ and w.l.o.g. we can assume $n_1 \le \ldots \le n_u$. In our situation we choose a prime $p \nmid \mathrm{disc}(f)$ to obtain a congruence factorization $f \equiv f_1 \cdot \ldots \cdot f_u \bmod p\mathbb{Z}[t]$. It follows that $n_i \, (i = 1, \ldots, u)$ coincides with the degree of the polynomial f_i. The cycles π_i permute the roots of f_i.

Example 2.6. *Let $f(t) = t^4 + 2$ be a generating polynomial of K and $G = \mathrm{Gal}(f)$.*

1 $f(t) \equiv t^4 \bmod 2$.
2 $f(t) \equiv (t+2)(t+1)(t^2+1) \bmod 3$.
3 $f(t) \equiv t^4 + 2 \bmod 5$.
4 $f(t) \equiv (t^2 + 6t + 4)(t^2 + t + 4) \bmod 7$.

Let p denote the modulus. In the first case p divides the discriminant and the van der Waerden criterion is of no use. In the other cases we get cycles of cycle type $[1, 1, 2]$, $[4]$ and $[2, 2]$. In all of these cases the roots can only be identified modulo p in a suitable finite field.

Definition 2.7. *Let $\pi \in G$ be as above with $|\pi_i| = n_i$ $(1 \le i \le u)$ and $H = \langle \pi \rangle$. A subset A of Ω consisting of d elements is called a* **potential block** *of size d, if $A^{\pi^j} \cap A \in \{\emptyset, A\}$ for $1 \le j \le |H|$. A system $A_1, \ldots, A_m$ of potential blocks of size d is called a* **potential block system** *if the union of that system is Ω, any two distinct elements of that system are disjoint, and $A_i^{\pi^j}$ $(1 \le j \le |H|, 1 \le i \le m)$ also belongs to that system.*

Remark 2.8. *The definitions potential block and potential block system depend on H. It is easy to see that all blocks are also potential blocks and all block systems are also potential block systems.*

Theorem 2.9. *Let $H = \langle \pi \rangle$ be a subgroup of G, A be a potential block and k be the smallest positive integer with $A^{\pi^k} = A$. If a cycle π_l of length n_l contains an element of A, then k divides n_l and π_l contains exactly $\frac{n_l}{k}$ elements of A.*

Proof. Since A is a potential block there is some positive integer k for which

$$A^{\pi^j} \cap A = \emptyset \text{ for } 1 \le j < k \text{ and } A^{\pi^k} = A.$$

Let α be an element which is contained in π_l and in A. It follows that all elements of the form $\alpha^{\pi^{ck}}$ $(c \in \mathbb{N})$ are contained in A, but all elements of the form $\alpha^{\pi^{ck+j}}$ $(c \in \mathbb{N}, 1 \le j < k)$ are not contained in A. Because $\alpha^{\pi^{n_l}} = \alpha$, it follows that k divides n_l and π_l contains exactly $\frac{n_l}{k}$ elements of A. $\square$

We call the integer k in the theorem above the **exponent** of the potential block A.

Theorem 2.10. *Let $H = \langle \pi \rangle$ be a subgroup of G and $A_1, \ldots, A_m$ be a potential block system with exponents $k_1, \ldots, k_m$. If A_i and A_j contain elements of the same cycle, it follows that $k_i = k_j$. In this case A_i contains an element of the cycle π_μ $(1 \le \mu \le u)$ if and only if A_j contains an element of π_μ.*

Proof. By assumption there exists a smallest positive integer c with $A_i^{\pi^c} \cap A_j \ne \emptyset$. Since $A_i^{\pi^c}$ is a potential block which belongs to the potential block system $A_1, \ldots, A_m$, it follows that $A_i^{\pi^c} = A_j$. $\square$

The last two theorems are important for calculating potential block systems. We construct systems of subsets $A_1, \ldots, A_m$ of Ω and integers $k_1, \ldots, k_m$ with the following properties:

1 $|A_i| = d \in \mathbb{N}$ for $1 \le i \le m$.
2 If A_i contains an element of a cycle π_l, then A_i contains exactly $\frac{n_l}{k_i}$ elements of π_l.
3 $\bigcup_{1 \le i \le m} A_i = \Omega$.
4 $A_i \cap A_j = \emptyset$ for $i \ne j$.
5 If A_i and A_j contain elements of the same cycle, it follows that $k_i = k_j$ and $A_i = A_j^{\pi^\mu}$ for a suitable $1 \le \mu \le k_i$.

We note that a system of subsets $A_1, \ldots, A_m$ of Ω with the above properties is a potential block system.

ALGORITHM 2.11. (Computation of potential block systems)

Input: *A generating polynomial f of K, a size d and a prime $p \nmid disc(f)$.*

Output: *A list of all potential block systems of blocks of size d.*

Step 1: *Compute the congruence factorization $f(t) \equiv f_1 \cdot \ldots \cdot f_r \bmod p\mathbb{Z}[t]$.*

Step 2: *Set $n_i = \deg(f_i)$ and compute a root α_i of f_i in a suitable extension of $\mathbb{F}_p$ $(1 \leq i \leq r)$.*

Step 3: *Set the cycle $\pi_i = (\alpha_i \; \alpha_i^p \ldots \alpha_i^{p^{n_i-1}})$ $(1 \leq i \leq r)$.*

Step 4: *Set $Z = \{\pi_1, \ldots, \pi_r\}$ and call CalcBlock($Z, d, \emptyset$).*

SUBALGORITHM 2.12. (CalcBlock)

Input: *A set Z consisting of cycles, a size d and a set Y.*

Output: *A list of potential block systems of size d.*

Step 1: *Set $k = 1$, $r = |Z|$ and let $n_1, \ldots, n_r$ be the lengths of the cycles contained in Z.*

Step 2: *Determine all subsets B of $\{2, \ldots, r\}$ satisfying $dk - n_1 = \sum_{b \in B} n_b$ and $k \mid n_b$ for all $b \in B$. For each such subset B do:*

(i) Set $Z' = \{\pi_1\}$ and add the cycles belonging to B to Z'.
(ii) Add Z' to Y.
(iii) If $Z = Z'$ call PrintBlockSystem(Y', d)
else call CalcBlock($Z \setminus Z', d, Y$)
(iv) Remove Z' from Y.

Step 3: *For $k = n_1$ terminate. Else increase k to the smallest divisor of n_1 bigger than k and go to Step 2.*

SUBALGORITHM 2.13. (PrintBlockSystem)

Input: *A set Y consisting of sets of cycles and a block size d.*

Output: *A list of potential block systems of size d belonging to Y.*

Step 1: *Set $\Delta = \emptyset$, $r = |Y|$ and let $Y_1, \ldots, Y_r$ be the elements of Y.*

Step 2: *For $i = 1, \ldots, r$ do*

(i) Set $s_i = |Y_i|$ and let $\pi_1, \ldots, \pi_{s_i}$ be the elements of Y_i.
(ii) Set $n_j = |\pi_j|$ $(1 \leq j \leq s_i)$ and $k_i = \frac{1}{d} \sum_{j=1}^{s_i} n_j \in \mathbb{N}$.
(iii) Let α_j be a fixed element of the cycle π_j $(1 \leq j \leq s_i)$.
(iv) Set $\Delta_1, \ldots, \Delta_{k_i} = \emptyset$.
(v) Add $\alpha_j^{\pi_j^l}$ to $\Delta_{l \bmod k_i}$ $(1 \leq j \leq r,\ 1 \leq l \leq n_j,\ l \bmod k_i \in \{1, \ldots, k_i\})$.
(vi) Add $\Delta_1, \ldots, \Delta_{k_i}$ to Δ.

Step 3: *Let $\pi_{i,1}, \ldots, \pi_{i,s_i}$ be the elements of Y_i, $(1 \leq i \leq r)$.*

Step 4: *Set $M = \{\prod_{i=1}^{r} \prod_{j=2}^{s_i} \pi_{i,j}^{e_{i,j}} \mid 1 \leq i \leq r,\ 2 \leq j \leq s_i,\ 0 \leq e_{i,j} < k_i\}$.*

Step 5: *For each $\tau \in M$ print the potential block system $\tau\Delta$.*

EXAMPLE 2.14. *Let $\pi \in G$ be of cycle decomposition $\pi = \pi_1\pi_2 = (\alpha_1\alpha_2)(\alpha_3\alpha_4)$ of lengths $n_i = 2$ $(i = 1, 2)$. For $k = 1$ the algorithm produces the potential block system $\{\alpha_1, \alpha_2\}, \{\alpha_3, \alpha_4\}$, and for $k = 2$ it produces two more potential block systems, namely $\{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_4\}$ and $\{\alpha_1, \alpha_4\}, \{\alpha_2, \alpha_3\}$.*

EXAMPLE 2.15. *Let $K = \mathbb{Q}(i\sqrt[6]{108})$ and $f(t) = t^6 + 108$. The polynomial $f(t)$ has the following congruence factorizations:*

$$\begin{aligned} f(t) &\equiv (t^2+2)(t^2+t+2)(t^2+4t+2) \bmod 5 \\ f(t) &\equiv (t^3+2)(t^3+5) \bmod 7 \\ f(t) &\equiv (t+3)(t+13)(t+15)(t+16)(t+18)(t+28) \bmod 31. \end{aligned}$$

From this information, we know that G contains elements of cycle types $[2, 2, 2], [3, 3]$, and $[1, 1, 1, 1, 1, 1]$. Choosing $p = 7$ and $\pi = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5, \alpha_6)$, we search for potential blocks of size 2. For $k = 1$ there is no subset B satisfying the condition in Step 3 of the algorithm, so k is set to 3. Combining one zero of π_1 with one zero of π_2, we get the conjugated potential blocks by the condition $A_{i+1} = A_1^{\pi^i}$ $(i = 1, 2)$. The algorithm prints the following potential block systems: $\{\{\alpha_1, \alpha_4\}\{\alpha_2, \alpha_5\}\{\alpha_3, \alpha_6\}\}$ $\{\{\alpha_1, \alpha_5\}\{\alpha_2, \alpha_6\}\{\alpha_3, \alpha_4\}\}$ $\{\{\alpha_1, \alpha_6\}\{\alpha_2, \alpha_4\}\{\alpha_3, \alpha_5\}\}$.

3. Computation of generating polynomials

In this section we construct a generating polynomial of the subfield L using the information we get from a potential block system. First we must determine whether the potential block system is a block system. In order to accomplish this, it becomes necessary to work in a suitable finite field $\mathbb{F}_q$, in which the zeros of f modulo p can be identified. It is known that exactly one unramified extension $\mathcal{F}$ of the p-adic field $\mathbb{Q}_p$ with residue class field $\mathbb{F}_q$ exists. In such a p-adic field we are able to identify the zeros of f.

Let $A_1, \ldots, A_m$ be a block system of G and $\beta_i := \prod_{\alpha \in A_i} \alpha \in N$. The problem is to determine the polynomial

$$g(t) = \prod_{i=1}^{m} (t - \beta_i) \in \mathbb{Z}[t].$$

Now let $\tilde{f}$ be the canonical embedding of f in $\mathbb{Z}_p$ and $\tilde{\alpha_1}, \ldots, \tilde{\alpha_n}$ be the zeros of $\tilde{f}$ in a suitable extension $\mathcal{E}$ of $\mathbb{Q}_p$. Set $\tilde{\beta}_i := \prod_{\tilde{\alpha} \in A_i} \tilde{\alpha} \in \mathcal{E}$ and calculate the polynomial

$$\tilde{g}(t) = \prod_{i=1}^{m} (t - \tilde{\beta}_i) \in \mathcal{E}[t].$$

THEOREM 3.1. *Let $A_1, \ldots, A_m$ be a complete block system and g and $\tilde{g}$ be as above. Then $\tilde{g} \in \mathbb{Z}_p[t]$ and if g is embedded into $\mathbb{Z}_p[t]$ in a canonical way, it follows that $g = \tilde{g}$.*

PROOF. Let $N = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ be the splitting field of f and $\mathfrak{p}$ be a prime ideal lying over p. Define $\phi : N \to N_{\mathfrak{p}}$ to be the canonical embedding. From this it is clear that $\phi(g) = \tilde{g}$. Since $\mathbb{Z} \subset \mathbb{Z}_p$ and $\mathcal{E} \subseteq N_{\mathfrak{p}}$, the theorem is proved. □

If we only assume that $A_1, \ldots, A_m$ is a potential block system it can be proved that

$\tilde{g} \in \mathbb{Z}_p[t]$. In practice we are able to do arithmetic in p-adic fields only modulo $\mathfrak{p}^k$ ($k \in \mathbb{N}$) up to some exponent, where $\mathfrak{p}$ is the prime ideal of the given p-adic field.

THEOREM 3.2. *Let $g, \tilde{g}, \tilde{\beta}_i$ $(1 \le i \le m), \mathcal{E}$ be defined as above, $k \in \mathbb{N}$ and $\mathfrak{p}$ the prime ideal of $\mathcal{E}$. Assume $\bar{\beta}_i \equiv \tilde{\beta}_i \bmod \mathfrak{p}^k$ $(1 \le i \le m)$ and define $\bar{g}(t) = \prod_{i=1}^m (t - \bar{\beta}_i)$. Then it follows that $\bar{g} \equiv \tilde{g} \bmod p^k$, hence $\bar{g} \equiv g \bmod p^k$.*

PROOF. Because of the definition of $\bar{g}$, we have $\bar{g} \equiv \tilde{g} \bmod \mathfrak{p}^k$. W.l.o.g. we can choose $\bar{g} \in \mathbb{Z}_p[t]$ and obtain $\bar{g} \equiv \tilde{g} \bmod p^k$. □

The next algorithm requires a bound M for the coefficients of the generating polynomial g, which is provided by the following lemma.

LEMMA 3.3. *Let f, g be as above and assume that g generates a subfield L of K. If $g(t) = \sum_{i=1}^m b_i t^i$ and $B = \prod_{i=1}^n \max(1, |\alpha_i|)$, then the following inequality holds:*

$$|b_i| \le \binom{m-1}{i-1} B + \binom{m-1}{j}.$$

PROOF. This is an immediate consequence of lemma 3.5.2 in Cohen (1993). □

ALGORITHM 3.4. (Computation of candidates for subfields)

Input: *A generating polynomial $f \in \mathbb{Z}[t]$ for K of degree n and a prime number p with a potential block system $A_1, \ldots, A_m$. A bound M for the coefficients of the generating polynomial g of the potential subfield L.*

Output: *A generating polynomial g for a potential subfield L of degree m.*

Step 1: *Determine the exponents k_i of A_i for $1 \le i \le m$ from the congruence factorization of f modulo $p\mathbb{Z}[t]$.*

Step 2: *For $1 \le i \le m$ calculate the cycles and corresponding polynomials which contain elements in A_i, factorize these polynomials in an extension of degree k_i of $\mathbb{F}_p$ and determine the zeros belonging to A_i.*

Step 3: *Factorize f in an extension of degree $k = \mathrm{lcm}(k_1, ..., k_m)$ of $\mathbb{F}_p$.*

Step 4: *Lift those factors to a sufficient precision ($> 2M$) by Hensel's method.*

Step 5: *Compute $\mathfrak{p}$–adic approximations δ_i of the product of the zeros belonging to block A_i.*

Step 6: *Compute $g(t) = \prod_{i=1}^m (t - \delta_i)$.*

If the coefficients of g are bigger than the bound M, it was previously shown that $A_1, \ldots, A_m$ is a potential but not a complete block system. If the polynomial g has multiple roots, a suitable Tschirnhausen transformation must be applied to f and the algorithm (with new bound M) is repeated.

We remark that Step 4 is not done for each potential block system. We can store the Hensel lifting and use it again for further potential block systems.

Example 3.5. *Let* $K = \mathbb{Q}(i\sqrt[6]{108})$, $f(t) = t^6 + 108$ *and* $p = 7$. *In example 2.15 three potential block systems were computed. The exponents of all blocks are 3. We generate a p-adic field* $\mathcal{E}/\mathbb{Q}_7$ *by a zero* γ *of the polynomial* $\omega(t) = t^3 + 6t^2 + 4$. *Let* $\mathfrak{p}$ *be the prime ideal in* $\mathcal{E}$. *We get the following congruence factorization (with* $[a, b, c]$ *representing* $a + b\gamma + c\gamma^2 \in \mathbb{Z}_p + \mathbb{Z}_p\gamma + \mathbb{Z}_p\gamma^2 = o_{\mathcal{E}}$*):*

$$\begin{aligned} f(t) \equiv\ & (t - [204, 408, 51])(t - [-101, -202, 575])(t - [-103, -206, -626]) \\ & (t - [101, 202, -575])(t - [103, 206, 626])(t - [-204, -408, -51]) \bmod \mathfrak{p}^4. \end{aligned}$$

The factors are sorted according to the Frobenius automorphism. In the notation of example 2.15 we obtain:

$$\alpha_1 = [204, 408, 51], \alpha_2 = [-101, -202, 575], \alpha_3 = [-103, -206, -626],$$

$$\alpha_4 = [101, 202, -575], \alpha_5 = [103, 206, 626], \alpha_6 = [-204, -408, -51].$$

It is now possible to compute $\delta_1, \delta_2, \delta_3$ *and the polynomial* $g(t) = \prod_{i=1}^{3}(t - \delta_i)$ *for each potential block system. In all cases we get* $g(t) = t^3 - 108 \bmod p^4$. *Then embeddings need to be computed in order to determine whether these polynomials generate subfields of* K.

4. Embedding of Subfields

The embedding of the computed potential subfields is a modification of Dixon's algorithm (1990). The advantage of our method is that we do not have to try several partitions of roots because we work with a potential block system.

Algorithm 4.1. (Embedding of potential subfields)

Input: *A generating polynomial* $f \in \mathbb{Z}[t]$ *for* K *of degree* n, *and a polynomial* g *generated by Algorithm 3.4 with corresponding prime number* p *and potential block system* $A_1, \ldots, A_m$.

Output: *A polynomial* $h \in \mathbb{Q}[t]$ *satisfying* $g(h) \equiv 0 \mod f\mathbb{Z}[t]$ *if* g *is a generating polynomial of a subfield of* K, *or the result that* $A_1, \ldots, A_m$ *is not a block system.*

Step 1: *Calculate* $h_0 \in \mathbb{Z}[t]$ *satisfying* $h_0(\alpha_j) \equiv \beta_i \bmod p$ *for all* $\alpha_j \in A_i$ $(1 \le i \le m)$.

Step 2: *Lift* h_0 *to a sufficient precision* h_k *modulo* p^{2^k} *by Newton's method.*

Step 3: *Retrieve from* h_k *a polynomial* $h \in \mathbb{Q}(t)$. *If* f *divides* $g(h)$ *print* h, *else print "*g *does not generate a subfield of* K*".*

A bound for Step 2 can be found in Dixon (1990). It seems that these bounds usually grossly overestimate the size of the numerators and denominators of the coefficients of h. One possibility is to check if the condition $g(h) \equiv 0 \bmod f\mathbb{Z}[t]$ is fulfilled after each iteration of the Newton lifting, but the calculation of $g(h)$ is expensive. Another possibility is to calculate only $h \in \mathbb{Q}[t]$ after each iteration and compare this with the h calculated one iteration before. We only check $g(h) \equiv 0 \bmod f\mathbb{Z}[t]$ if h remains invariant.

Example 4.2. *We conclude examples 2.15,3.5 using the methods described in Dixon*

(1990) to compute $h \bmod p$. *In the first case we get* $h(t) \equiv 4t^5 + 4t^2 \bmod 7$ *and by the Newton lifting method,*

$$\begin{aligned} h(t) &\equiv 10123920347235939257798576 01 \cdot t^5 \\ &+ 5522138371219603231526496 01 \cdot t^2 \bmod 7^{32}. \end{aligned}$$

Retrieving the coefficients in $\mathbb{Q}$, *we get* $h(t) = -\frac{1}{12}t^5 + \frac{1}{2}t^2$. *In the two other cases:*

$$\begin{aligned} h(t) &\equiv 1012392034723593925779857601 \cdot t^5 \\ &+ 552213837121960323152649601 \cdot t^2 \bmod 7^{32}, \end{aligned}$$

whence $h(t) = \frac{1}{12} \cdot t^5 + \frac{1}{2} \cdot t^2$, *furthermore,*

$$h(t) \equiv 1104427674243920646305299200 \cdot t^2 \bmod 7^{32},$$

from which $h(t) = -t^2$ *follows.*

The condition $f \mid g(h)$ *is fulfilled in all cases.*

5. The Algorithm

ALGORITHM 5.1. (Calculation of subfields)

Input: *A generating polynomial* $f \in \mathbb{Z}[t]$ *for* K *of degree* n.

Output: *A list of characterizing pairs* (h, g) *of all non-trivial subfields* L *of* K. *For all* $d \mid n \; (d \neq 1, d \neq n)$ *do*

Step 1: *Choose several primes* $p \nmid \operatorname{disc}(f)$ *and use algorithm 2.11 to compute a list of potential block systems.*

Step 2: *Choose a prime* p *and the corresponding list of potential block systems which appear to be most suitable.*

Step 3: *For all potential block systems of that list use algorithm 3.4 to compute potential generating polynomials.*

Step 4: *For all those potential generating polynomials use algorithm 4.1 to compute an embedding or decide that the potential block system was not a complete block system.*

It is difficult to say which prime is the best one in Step 2. On the one hand we want to choose a prime for which the number of potential block systems is small, on the other hand it is faster to do arithmetic in p-adic fields of small degree. There are two ways of detecting potential block systems which are not complete block systems. The first one is that the coefficients of g are bigger than the bound M. The other one is very expensive because we try in Step 4 to compute an embedding which does not exist. In most cases it is better to choose a larger bound (for example M^2 or M^4) in Step 4 of Algorithm 3.4 because there is a better chance of finding that the coefficients of g are too big.

The algorithm to compute generating polynomials of subfields is a generalization of the method presented in Dixon (1990). Dixons algorithm can only work with potential blocks of exponent 1. To compute all subfields of given degree m the algorithm has to find a prime p such that all potential blocks which contain α have exponent 1. In all algebraic number fields there exist primes which correspond to permutations of cycle

Table 1. Examples

No	Polynomial	Time
1	$t^6 + 108$	1.1 sec
2	$t^8 - 12t^6 + 23t^4 - 12t^2 + 1$	4.0 sec
3	$t^8 - 10t^4 + 1$	1.5 sec
4	$t^8 + 4t^6 + 10t^4 + 12t^2 + 7$	1.8 sec
5	$t^9 - 18t^8 + 117t^7 - 348t^6 + 396t^5 + 288t^4 + 3012t^3 + 576t^2 + 576t - 512$	3.3 sec
6	$t^{10} + 38t^9 - 99t^8 + 1334t^7 - 4272t^6 + 9244t^5 - 8297t^4 + 1222t^3 + 1023t^2 - 74t + 1$	3.4 sec
7	$t^{10} - 20t^9 + 80t^8 + 200t^7 - 3770t^6 + 872t^5 + 29080t^4 + 36280t^3 - 456615t^2 + 541260t - 517448$	3.9 sec
8	$t^{10} - 10t^8 + 20t^7 + 235t^6 + 606t^5 + 800t^4 + 600t^3 + 270t^2 + 70t + 16$	3.2 sec
9	$t^{12} + 6t^9 + 4t^8 + 8t^6 - 4t^5 - 12t^4 + 8t^3 - 8t + 8$	7.4 sec
10	$t^{12} + 9t^{11} + 3t^{10} - 73t^9 - 177t^8 - 267t^7 - 315t^6 - 267t^5 - 177t^4 - 73t^3 + 3t^2 + 9t + 1$	14 sec
11	$t^{12} - 34734t^{11} + 401000259t^{10} - 1456627492885t^9 - 2537142937228035t^8 + 18762072755679375516t^7 - 812368636358864062944t^6 - 70132863629758257512231931t^5 + 25834472514893102332821062085t^4 + 76623280610352450247247939584745t^3 - 45080885015422662132515763499758450t^2 - 2070499552240812214288316981071818900t - 550505759097778545485364826246753544$	98 sec
12	$t^{15} + 20t^{12} + 125t^{11} + 503t^{10} + 1650t^9 + 3430t^8 + 4690t^7 + 4335t^6 + 2904t^5 + 1400t^4 + 485t^3 + 100t^2 + 15t + 1$	10 sec

type $[1, \dots, 1]$, but in this case the number of potential blocks of size d which contain α is equal to $\binom{n}{d}$. Another problem of Dixons algorithm is to check that a potential block is not a block. In this case Hensel lifting is used up to a bound which is much bigger than the $m-th$ power of the bound used in our algorithm. An important fact is that we lift the factors using Hensel lifting only once and save the congruence factorization. So for each block there are only a few multiplications in the p-adic field $\mathcal{E}$ neccessary to get the potential generating polynomial in comparison to Dixons method which reduces a lattice of degree m by the LLL-method presented in Lenstra, Lenstra, Lovász (1982).

6. Examples

Table 1 lists 12 examples of test polynomials and the computation times needed by our algorithm. A. Hulpke (1995) uses these examples to compare the algorithms presented in [Casperson, Ford, McKay (1995), Lazard, Valibouze (1993), Cohen, Diaz y Diaz (1991), Hulpke (1995)]. We remark that the algorithm presented in Cohen, Diaz y Diaz (1991) does in general not compute all subfields. Nevertheless in the more complicated examples our algorithm runs faster. In comparison with the other methods our algorithm runs always faster. The differences in compuations times become more significant if the examples become more complex. In the last two examples our algorithm is 173 resp. 1013 times faster than the best of the other ones.

Consider the algebraic number field K (Example 10) which is generated by the polynomial

$$f(t) = t^{12} + 9t^{11} + 3t^{10} - 73t^9 - 177t^8 - 267t^7 - 315t^6 - 267t^5 - 177t^4 - 73t^3 + 3t^2 + 9t + 1.$$

This example is taken from Lazard, Valibouze (1993). The authors use the fact that the polynomial f is reciprocal to find a subfield of degree 6. Then they only compute subfields of that subfield.

We note that all computed generating polynomials for subfields have the form $(t-1)^m$. Substituting $t = t+1$ in f we obtain the following generating polynomials:

(i) $t^6 - 21t^5 + 147t^4 - 378t^3 + 1323t - 1323$ with zero $11 + 2\alpha - 73\alpha^2 - 177\alpha^3 - 267\alpha^4 - 315\alpha^5 - 267\alpha^6 - 177\alpha^7 - 73\alpha^8 + 3\alpha^9 + 9\alpha^{10} + \alpha^{11}$.

(ii) $t^4 - 63t^2 - 1323$ with zero $\frac{1}{63}(995 + 2372\alpha - 10873\alpha^2 - 32232\alpha^3 - 50058\alpha^4 - 63357\alpha^5 - 55881\alpha^6 - 38445\alpha^7 - 18255\alpha^8 + 16\alpha^9 + 2188\alpha^{10} + 253\alpha^{11})$.

(iii) $t^3 - 21t^2 + 1323$ with zero $\frac{1}{21}(282 - 556\alpha - 2012\alpha^2 - 2562\alpha^3 - 3405\alpha^4 - 2772\alpha^5 - 1743\alpha^6 - 849\alpha^7 + 234\alpha^8 + 171\alpha^9 - 14\alpha^{10} - 4\alpha^{11})$.

(iv) $t^2 + 63t - 1323$ with zero $\frac{1}{3}(-222 + 130\alpha - 115\alpha^2 - 1062\alpha^3 - 1566\alpha^4 - 2667\alpha^5 - 2583\alpha^6 - 1983\alpha^7 - 1341\alpha^8 - 102\alpha^9 + 152\alpha^{10} + 19\alpha^{11})$.

Finally we present two more examples. Consider the algebraic number field K generated by the polynomial

$$f(t) = t^{12} + t^{11} - 28t^{10} - 40t^9 + 180t^8 + 426t^7 + 89t^6 - 444t^5 - 390t^4 - 75t^3 + 27t^2 + 11t + 1.$$

K is a Galois extension of $\mathbb{Q}$ with Galois group $\mathfrak{A}_4$. We know that K has three subfields of degree 6, four of degree 4, and one of degree 3.

The following subfields are calculated:

(i) $t^6 - 6t^5 - 2t^4 + 48t^3 - 45t^2 - 22t + 1$ with zero $\frac{1}{196}(197\alpha^{11} + 215\alpha^{10} - 5664\alpha^9 - 8255\alpha^8 + 39260\alpha^7 + 85688\alpha^6 - 4800\alpha^5 - 102279\alpha^4 - 52471\alpha^3 + 3646\alpha^2 + 4797\alpha + 558)$.

(ii) $t^6 - 3t^5 - 11t^4 + 27t^3 - 3t^2 - 11t + 1$ with zero $\frac{1}{196}(-433\alpha^{11} - 443\alpha^{10} + 12200\alpha^9 + 17603\alpha^8 - 79964\alpha^7 - 187354\alpha^6 - 25898\alpha^5 + 211713\alpha^4 + 158845\alpha^3 + 9988\alpha^2 - 16091\alpha - 2620)$.

(iii) $t^6 - 24t^5 + 211t^4 - 816t^3 + 1282t^2 - 528t - 241$ with zero $\frac{1}{196}(3473\alpha^{11} + 40546\alpha^{10} + 116829\alpha^9 - 307383\alpha^8 - 2296210\alpha^7 - 3295368\alpha^6 + 10194228\alpha^5 + 21948643\alpha^4 + 27601378\alpha^3 + 14431917\alpha^2 + 1621177\alpha - 658412)$.

(iv) $t^4 - 24t^3 + 38t^2 + 16t + 1$ with zero $\frac{1}{14}(-83\alpha^{11} + 29\alpha^{10} + 2287\alpha^9 + 229\alpha^8 - 15304\alpha^7 - 14599\alpha^6 + 12655\alpha^5 + 19396\alpha^4 + 5550\alpha^3 - 888\alpha^2 - 658\alpha - 14)$.

(v) $t^4 - 7t^3 + 5t^2 + 6t + 1$ with zero $\frac{1}{196}(-953\alpha^{11} - 1258\alpha^{10} + 27084\alpha^9 + 46419\alpha^8 - 178833\alpha^7 - 462883\alpha^6 - 83043\alpha^5 + 519472\alpha^4 + 389689\alpha^3 + 23745\alpha^2 - 38628\alpha - 6326)$.

(vi) $t^4 - 28t^3 - 15t^2 + 3t + 1$ with zero $\frac{1}{196}(256\alpha^{11} + 244\alpha^{10} - 7207\alpha^9 - 9906\alpha^8 + 47336\alpha^7 + 107223\alpha^6 + 12041\alpha^5 - 120443\alpha^4 - 88903\alpha^3 - 6678\alpha^2 + 8709\alpha + 1525)$.

(vii) $t^4 - 10t^3 - 32t^2 + 410t - 241$ with zero
$4\alpha^{11} + 46\alpha^{10} + 128\alpha^9 - 362\alpha^8 - 2560\alpha^7 - 3524\alpha^6 + 5848\alpha^5 + 24142\alpha^4 + 30082\alpha^3 + 15750\alpha^2 + 1804\alpha - 723$.

(viii) $t^3 + 14t^2 + 11t - 1$ with zero
$\frac{1}{196}(670\alpha^{11} + 165\alpha^{10} - 18884\alpha^9 - 12568\alpha^8 + 130059\alpha^7 + 187423\alpha^6 - 81449\alpha^5 - 236127\alpha^4 - 84296\alpha^3 + 11769\alpha^2 + 8375\alpha + 886)$.

We remark that K is the Hilbert class field of all subfields except the ones of degree 4. The computations are done in 11 seconds.

As a last example consider the algebraic number field K generated by a root of $f(t) = t^{24} + 8t^{23} - 32t^{22} - 298t^{21} + 624t^{20} + 4592t^{19} - 8845t^{18} - 31488t^{17} + 76813t^{16} + 65924t^{15} - 265616t^{14} + 48348t^{13} + 385639t^{12} - 394984t^{11} - 20946t^{10} + 369102t^9 - 362877t^8 + 183396t^7 + 434501t^6 - 194418t^5 + 450637t^4 + 125800t^3 - 16401t^2 - 45880t + 115151$.

This field is normal and has Galois group $\mathfrak{S}_4$. All subfields are computed in 3641 seconds. In the following we give only the generating polynomials for the subfields. We remark that the embeddings are calculated, too.

(i) $t^{12} - 64t^{11} + 1528t^{10} - 16044t^9 + 74871t^8 - 161098t^7 + 167141t^6 - 165210t^5 + 297029t^4 - 337174t^3 + 250670t^2 - 232280t + 115151$

(ii) $t^{12} - 16t^{11} + 108t^{10} - 497t^9 + 1272t^8 + 696t^7 - 6462t^6 + 11299t^5 + 40150t^4 - 91516t^3 + 117738t^2 + 60955t + 115151$

(iii) $t^{12} - 16t^{11} + 96t^{10} - 360t^9 + 1611t^8 - 586t^7 + 14297t^6 + 61286t^5 + 171105t^4 + 391026t^3 + 566042t^2 + 406920t + 115151$

(iv) $t^{12} + 12t^{11} + 66t^{10} + 126t^9 - 197t^8 + 448t^7 + 13451t^6 + 45368t^5 + 40519t^4 + 58994t^3 + 345440t^2 + 289742t + 115151$

(v) $t^{12} + 12t^{11} + 66t^{10} + 235t^9 + 990t^8 + 3810t^7 + 13828t^6 + 51693t^5 + 154690t^4 + 325806t^3 + 446598t^2 + 343639t + 115151$

(vi) $t^{12} - 64t^{11} + 1502t^{10} - 16240t^9 + 90981t^8 - 256278t^7 + 307603t^6 - 45436t^5 - 422451t^4 + 596072t^3 - 38966t^2 - 330506t + 115151$

(vii) $t^{12} - 16t^{10} - 80t^9 + 375t^8 + 4686t^7 + 21445t^6 + 79986t^5 + 221445t^4 + 534570t^3 + 960134t^2 + 596720t + 115151$

(viii) $t^{12} + 16t^{10} - 79t^9 + 389t^8 + 1480t^7 + 5387t^6 + 18142t^5 + 62659t^4 - 34301t^3 + 8181t^2 - 167175t + 115151$

(ix) $t^{12} - 64t^{11} + 1386t^{10} - 12910t^9 + 58159t^8 - 149404t^7 + 321179t^6 - 533388t^5 + 699503t^4 - 782862t^3 + 588268t^2 - 407282t + 115151$

(x) $t^8 + 66t^7 + 1665t^6 + 15423t^5 + 82484t^4 + 180311t^3 + 256795t^2 + 230941t + 115151$

(xi) $t^8 + 66t^7 + 1603t^6 + 17522t^5 + 87416t^4 + 178964t^3 + 218318t^2 + 184564t + 115151$

(xii) $t^8 + 84t^7 + 2043t^6 + 7800t^5 + 4523t^4 - 76082t^3 + 250207t^2 + 121808t + 115151$

(xiii) $t^8 + 36t^7 + 799t^6 + 8903t^5 + 67422t^4 + 156757t^3 + 182615t^2 + 32205t + 115151$

(xiv) $t^6 - 12t^5 + 117t^4 - 23296t^3 + 83483t^2 - 68948t + 115151$

(xv) $t^6 + 28t^5 - 45t^4 - 10361t^3 + 63645t^2 + 49178t + 115151$

(xvi) $t^6 - 31t^5 + 1054t^4 + 5482t^3 - 39876t^2 - 257589t + 115151$

(xvii) $t^6 - 11t^5 + 1135t^4 + 5420t^3 - 14079t^2 - 182673t + 115151$

(xviii) $t^6 - 57t^5 + 210t^4 - 1896t^3 + 13010t^2 + 89517t + 115151$

(xix) $t^6 - 49t^5 + 697t^4 - 5202t^3 + 38951t^2 - 104893t + 115151$

(xx) $t^6 - 2260t^5 + 258433t^4 - 8759552t^3 + 89549811t^2 - 190825164t + 77649707$

(xxi) $t^4 + 17t^3 + 595t^2 + 15905t + 115151$
(xxii) $t^4 - 31t^3 + 1004t^2 - 14302t + 115151$
(xxiii) $t^4 - 85t^3 + 2392t^2 - 24634t + 115151$
(xxiv) $t^4 - 55t^3 + 2158t^2 - 26278t + 115151$
(xxv) $t^3 - 853t^2 + 74371t - 115151$
(xxvi) $t^3 - 1253t^2 + 44579t - 115151$
(xxvii) $t^3 - 2525t^2 + 112131t - 918751$
(xxviii) $t^2 - 45252t + 115151$

All computations were done on a HP 9000/735 in KASH [Daberkow, Fieker, Klüners, Pohst, Roegner, Schörnig, Wildanger (1995)], the shell of KANT V4.

References

Casperson, D., Ford, D., McKay, J. (1995). An ideal decomposition algorithm. *Submitted to J. Symb. Comput.*

Cohen, H. (1993). A Course in Computational Algebraic Number Theory. *Berlin - Heidelberg - New York: Springer–Verlag.*

Cohen, H., Diaz y Diaz, F. (1991). A polynomial reduction algorithm. *Seminaire de Theorie des Nombres de Bordeaux (Serie 2)* **3**, *351-360.*

Dixon, J. (1990). Computing Subfields in Algebraic Number Fields. *J. Austral. Math. Soc. (Series A)* **49**, *434–448.*

Hulpke, A. (1995). Block Systems of a Galois Group. *Exp. Math. 4, No. 1, 1-9 (1995).*

Daberkow, M., Fieker, C., Klüners, J., Pohst, Roegner, K., Schörnig, M., Wildanger, K. (1995). KANT V4. *Submitted to J. Symb. Comput.*

Landau,S., Miller, G.L. (1985). Solvability by Radicals Is in Polynomial Time. *J. of Computer and System Sciences* **30**, *179–208.*

Lazard, D., Valibouze, A. (1993). Computing subfields: Reverse of the primitive element problem. *In: F. Eyssete, A. Galligo, editors, MEGA-92, Computational algebraic geometry, Vol. 109 of Progress in Mathematics, 163–176, Birkhäuser, Boston.*

Lenstra, A.K., Lenstra, H.W., Lovász, L. (1982). Factoring Polynomials with Rational Coefficients. *Math.Ann.* **261**, *515–534.*

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

Wielandt, H. (1964). Finite Permutation Groups. *New York and London:Academic Press.*