ON POLYNOMIAL DECOMPOSITIONS

JÜRGEN KLÜNERS
UNIVERSITÄT HEIDELBERG,
IM NEUENHEIMER FELD 368, 69120 HEIDELBERG, GERMANY
E-MAIL ADDRESS: KLUENERS@IWR.UNI-HEIDELBERG.DE

ABSTRACT. We present a new polynomial decomposition which generalizes the functional and homogeneous bivariate decomposition of irreducible monic polynomials in $\mathbb{Q}[t]$. With these decompositions it is possible to calculate the roots of an imprimitive polynomial by solving polynomial equations of lower degree.

1. INTRODUCTION

The purpose of this paper is to introduce the norm decomposition which enables us to compute the roots of a monic irreducible imprimitive polynomial $f \in \mathbb{Q}[t]$ by solving polynomial equations of lower degree. We call an irreducible polynomial f imprimitive if the number field generated by a root of f contains non–trivial subfields. We will see that for each subfield there exists a norm decomposition. The norm decomposition generalizes the functional [Kozen and Landau, 1989] and homogeneous bivariate decomposition [von zur Gathen and Weiss, 1995]. There exist imprimitive polynomials having neither a functional nor a homogeneous bivariate decomposition. However, these polynomials always have a norm decomposition. Furthermore, the computing times by our algorithm are much shorter than the ones for a homogeneous bivariate decomposition.

If a functional decomposition $f = g(h)$ with $g, h \in \mathbb{Q}[t]$ exists we can calculate the roots $\beta_1, \ldots, \beta_m$ of g, and then the roots of $h - \beta_i$ $(1 \leq i \leq m)$ in order to get the roots of f. Note that there are very efficient algorithms to compute functional decompositions.

In the homogeneous bivariate decomposition the polynomial f is written in the form $f = \hat{g}(h_1, h_2)$ where $\hat{g} \in \mathbb{Q}[t, u]$ is homogeneous and $h_1, h_2 \in \mathbb{Q}[t]$. A drawback of the known algorithms for computing a homogeneous bivariate decomposition is that they require an expensive factorization of the polynomial f in $K[t]$, where K is the number field generated by a root of f. If f has a homogeneous bivariate decomposition then $f = h_2^m g(\frac{h_1}{h_2})$, where $g(t) = \hat{g}(t, 1)$ and $m = \deg(\hat{g})$. Since f is irreducible we obtain the roots of f by first computing the roots $\beta_1, \ldots, \beta_m$ of g and then the roots of the polynomials $h_1 - \beta_i h_2$ $(1 \leq i \leq m)$.

It is well known that the existence of subfields $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ [Casperson et al., 1996, Dixon, 1990, Hulpke, 1995, Klüners and Pohst, 1997, Lazard and Valibouze, 1993] is equivalent to $f \mid g(h)$ where $f, g \in \mathbb{Q}[t]$ are the minimal polynomials of α resp. β, $h \in \mathbb{Q}[t], \deg(g) \leq \deg(f)$. This is a generalization of the functional decomposition. [Lazard and Valibouze, 1993] illustrate by an example how to represent the roots of f by a "nested" system of equations which can be obtained via computing subfields.

The functional decomposition of irreducible (and reducible) polynomials is very useful for many applications. There are very efficient algorithms in theory and practice [Kozen and Landau, 1989] to compute functional decompositions. It is possible to compute functional decompositions of polynomials of degree 100 in less than a minute.

We want to look at polynomials where no functional decomposition is possible. A first approach was done in [von zur Gathen and Weiss, 1995] who defined the homogeneous bivariate decomposition. They describe in section 2 applications to robotics, which was one motivation to look at decomposition algorithms. An other application given in their paper is the relation to decompositions of rational functions. The authors proved a connection between block systems and homogeneous bivariate decompositions. It happens that there are polynomials with non-trivial block systems but there exists no non-trivial homogeneous bivariate decomposition.

Our approach generalizes and improves the homogeneous bivariate decomposition in a way that for each block system there exists a norm decomposition. These decompositions can be computed in a very efficient way using the subfield algorithm presented in [Klüners and Pohst, 1997]. We remark that this algorithm is exponential time in the worst case. A lot of computed examples show that it works very well in practice. We will discuss the efficiency in section 6.

The norm decomposition is an important step to the solvability by radicals. Similar to [Landau and Miller, 1985] the problem is reduced to primitive extension. The reduction given in [Landau and Miller, 1985] is computed in polynomial time based on factorization algorithms. In practice this approach is limited to polynomials of small degree.

2. Preliminaries

Let $f \in \mathbb{Q}[t]$ be an irreducible monic polynomial of degree n, $K = \mathbb{Q}(\alpha)$, and α a root of f.

Definition 2.1. *Let $g \in \mathbb{Q}[t]$ be an irreducible monic polynomial with zeros $\beta = \beta_1, \ldots, \beta_m$, and $L = \mathbb{Q}(\beta)$ an algebraic number field. We define*

$$.^{(i)} : L \to \mathbb{Q}(\beta_i) : \sum_{j=0}^{m-1} b_j \beta^j \mapsto \sum_{j=0}^{m-1} b_j \beta_i^j \ (b_j \in \mathbb{Q}).$$

We extend this definition to the polynomial algebra:

$$.^{(i)} : L[t] \to \mathbb{Q}(\beta_i)[t] : \sum_{j=0}^{k} c_j t^j \mapsto \sum_{j=0}^{k} c_j^{(i)} t^j \ (c_j^{(i)} \in \mathbb{Q}(\beta_i)).$$

For $h \in L[t]$ we define the norm

$$N_L(h) := N_g(h) := \prod_{i=1}^{m} h^{(i)} \in \mathbb{Q}[t].$$

We remark that the norm of a polynomial $h \in L[t]$ does not depend on the choice of a basis of $L/\mathbb{Q}$.

Definition 2.2. *Let $f \in \mathbb{Q}[t]$ be an irreducible monic polynomial of degree n.*

1. *We call $f = g(h)$ with $g, h \in \mathbb{Q}[t]$ and $1 < \deg(g) < n$ a functional decomposition.*
2. *We call $f = \hat{g}(h_1, h_2)$ with homogeneous $\hat{g} \in \mathbb{Q}[t, u]$, $h_1, h_2 \in \mathbb{Q}[t]$, $\deg(h_i) \leq \frac{n}{m}$ $(i = 1, 2)$, and $1 < m = \deg(\hat{g}) < n$ a homogeneous bivariate decomposition.*
3. *We call $f = N_g(h)$ a (norm) decomposition if $g \in \mathbb{Q}[t]$ is irreducible with $1 < \deg(g) < n$ and $h \in L[t]$, where L is the number field generated by a zero of g.*

The functional decomposition can be regarded as a special case of a homogeneous bivariate decomposition ($h_2 = 1$).

Theorem 2.3. *The functional decomposition and the homogeneous bivariate decomposition of an irreducible monic polynomial $f \in \mathbb{Q}[t]$ are special cases of a norm decomposition.*

Proof. Let $f = g(h)$ with $g, h \in \mathbb{Q}[t]$ and β be a root of g. Then we get

$$f = g(h) = \prod_{i=1}^{m}(h - \beta^{(i)}) = N_g(h - \beta).$$

Assuming $g = g_1 g_2$ we get $f = g_1(h)g_2(h)$. Since f is irreducible we get g is irreducible.

Let $f = \hat{g}(h_1, h_2)$ be a homogeneous bivariate decomposition. Letting $g(t) = \hat{g}(t, 1)$ and $m = \deg(g)$ we get

$$f = h_2^m \cdot g(\frac{h_1}{h_2}).$$

Now f and h_2 have no common root since $\deg(h_2) < \deg(f)$, hence

$$g(\frac{h_1(\alpha)}{h_2(\alpha)}) = 0.$$

Thus there exists a root $\beta = \frac{h_1(\alpha)}{h_2(\alpha)}$ of g such that $h_1(\alpha) - \beta h_2(\alpha) = 0$. Let $\tilde{h} := h_1 - \beta h_2$ and $\tilde{g}$ be the minimal polynomial of β. Since α is a root of $N_{\tilde{g}}(\tilde{h}) \in \mathbb{Q}[t]$ we have $N_{\tilde{g}}(\tilde{h}) = f$. From $\deg(g)\deg(\tilde{h}) \leq \deg(f)$ and $\tilde{g} \mid g$ it follows that $\tilde{g} = g$, thus g is irreducible. □

In the next example we see that the norm decomposition is a strict generalization of the homogeneous bivariate and the functional decomposition. It is easy to see (Lemma 3.5) that norm decompositions of polynomials of degree 4 correspond to homogeneous bivariate decompositions.

Example 2.4. *Let $f(t) = t^6 - 12t^5 + 54t^4 - 134t^3 + 153t^2 - 162t + 81$. We get the norm decomposition $f = N_g(h)$, where $g(t) = t^3 - 18t^2 + 81t - 81$ and $h(t) = t^2 + \frac{36 - 30\beta + 2\beta^2}{9}t + \beta$ and β a zero of g. Using Lemmas 3.4 and 3.5 we see that there is neither a homogeneous bivariate nor a functional decomposition of f.*

Remark 2.5. *For $f = N_g(h)$ we can express the zeros of f in the following way: First we calculate the zeros $\beta_1, \ldots, \beta_m$ of g. In a second step we determine the zeros of $h^{(i)}$ $(1 \leq i \leq m)$. Instead of solving an equation of degree n we first solve an equation of degree m and then m equations of degree $\frac{n}{m}$.*

In the following we give a description of subfields $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\alpha)$. Let f and g be the minimal polynomials of α resp. β. Then the subfield $\mathbb{Q}(\beta)$ can be described by a pair (g, ω), where $\omega \in \mathbb{Q}[t]$ and $\omega(\alpha) = \beta$. We call ω the embedding polynomial (of $\mathbb{Q}(\beta)$ in $\mathbb{Q}(\alpha)$). If we replace ω with $\omega \bmod f$ we can suppose that $\deg(\omega) < \deg(f)$. The following Lemma is an immediate consequence.

Lemma 2.6. *Let $f, g \in \mathbb{Q}[t]$ be monic, irreducible polynomials and α, β be a root of f resp. g. For $\omega \in \mathbb{Q}[t]$ the following is equivalent:*

1. *$\mathbb{Q}(\beta)$ is a subfield of $\mathbb{Q}(\alpha)$ with $\omega(\alpha) = \beta$.*
2. *$f \mid g(\omega)$.*

[Klüners and Pohst, 1997] developed an efficient algorithm to compute all subfields of an algebraic number field $K = \mathbb{Q}(\alpha)$ given by the minimal polynomial f of α. Each subfield $L = \mathbb{Q}(\beta)$ is characterized by a pair of polynomials (g, ω) where $g \in \mathbb{Q}[t]$ is the minimal polynomial of β and $\omega \in \mathbb{Q}[t]$ is the embedding polynomial with $\omega(\alpha) = \beta$. We remark that the subfield algorithm [Klüners and Pohst, 1997] works for monic irreducible polynomials in $\mathbb{Z}[t]$. It can be extended to non-monic

irreducible polynomials in $\mathbb{Z}[t]$ which is equivalent to monic irreducible polynomials in $\mathbb{Q}[t]$.

3. Subfields and Decompositions

Using Lemma 2.6 we easily see that functional decomposition is a special case of subfield computation. In this section we prove that there is a correspondence between subfields and norm decompositions. Furthermore we give a method to compute a norm decomposition which corresponds to a given subfield.

Lemma 3.1. *Let $f, g \in \mathbb{Q}[t]$ be monic, irreducible polynomials and α, β be a root of f resp. g. Then the following is equivalent:*

1. *$\mathbb{Q}(\beta)$ is a subfield of $\mathbb{Q}(\alpha)$ and $h \in \mathbb{Q}(\beta)[t]$ is the minimal polynomial of α over $\mathbb{Q}(\beta)$.*
2. *$f = N_g(h)$.*

Proof. Let $\mathbb{Q}(\beta)$ be a subfield of $\mathbb{Q}(\alpha)$ and h be the minimal polynomial of α over $\mathbb{Q}(\beta)$. It follows that α is a zero of $N_g(h)$. Since $\deg(N_g(h)) = \deg(f)$ and both polynomials are monic it follows that $f = N_g(h)$.

Letting $f = N_g(h)$ it follows that $h(\alpha) = 0$. This implies that $\mathbb{Q}(\beta)$ is a subfield of $\mathbb{Q}(\alpha)$ and h is the minimal polynomial of α over $\mathbb{Q}(\beta)$. □

We have seen that to each subfield there corresponds a decomposition and vice versa. This leads to the following definition.

Definition 3.2. *We call two decompositions equivalent if they correspond to the same subfield.*

The next theorem enables us to compute a norm decomposition corresponding to a subfield in a very efficient way.

Theorem 3.3. *Let $L = \mathbb{Q}(\beta)$ be a subfield of $K = \mathbb{Q}(\alpha)$ and $f, g \in \mathbb{Q}[t]$ be the minimal polynomials of α resp. β. Let $\omega \in \mathbb{Q}[t]$ be the embedding polynomial with $\omega(\alpha) = \beta$. Define*

$$h := \gcd_{L[t]}(f, \omega - \beta).$$

Then $N_g(h)$ is a norm decomposition of f.

Proof. From $f(\alpha) = 0$ and $\omega(\alpha) - \beta = 0$ it follows that $h(\alpha) = 0$. The assertion follows if we know that h is the minimal polynomial of α over L. Since $h(\alpha) = 0$ it suffices to prove that $\deg(h) \leq [K : L]$. The only isomorphism from L to $\bar{\mathbb{Q}}$ which leaves β invariant is the identity because β is a primitive element of $L/\mathbb{Q}$. There are exactly $[K : L]$ isomorphisms from K to $\bar{\mathbb{Q}}$ which leave β invariant. Thus there exist exactly $[K : L]$ zeros $\tilde{\alpha}$ of f with $\omega(\tilde{\alpha}) = \beta$. Since $h \mid \omega - \beta$ this implies $\deg(h) \leq [K : L]$. □

We compute the greatest common divisor of polynomials over number fields by a modular algorithm presented in [Encarnación, 1995]. The previous theorem provides us with a decomposition of f from a subfield of K. It is interesting to note that we are able to compute a functional or homogeneous bivariate decomposition if it exists, in spite of the dependency on the generating polynomial g rather than the corresponding subfield. The following Lemma is an immediate consequence of Theorem 8 of [Kozen and Landau, 1989].

Lemma 3.4. *Let $f = N_g(h)$ be a norm decomposition. There exists an equivalent functional decomposition of f if and only if $\tilde{h} := h - h(0) \in \mathbb{Q}[t]$. In that case we obtain the functional decomposition $f = \tilde{g}(\tilde{h})$, where $\tilde{g}$ is the minimal polynomial of $h(0)$ over $\mathbb{Q}$.*

Lemma 3.5. *Let $f = N_g(h)$ be a norm decomposition. There exists an equivalent homogeneous bivariate decomposition if and only if $h = h_1 - \tilde{\beta} h_2$ with $h_i \in \mathbb{Q}[t]$ $(i = 1, 2)$, and $\tilde{\beta} \in L$. In this case let $\tilde{g}$ the minimal polynomial of $\tilde{\beta}$. Then $f = \hat{g}(h_1, h_2)$ is a homogeneous bivariate decomposition, where $\hat{g} \in \mathbb{Q}[t, u]$ is homogeneous and $\hat{g}(t, 1) = \tilde{g}(t)$.*

Proof. If f has an equivalent homogeneous bivariate decomposition it follows from the proof of Theorem 2.3 that $h = h_1 - \tilde{\beta} h_2$.

Now we assume that $h = h_1 - \tilde{\beta} h_2$. Let α be a zero of h. From

$$h(\alpha) = 0 = h_1(\alpha) - \tilde{\beta} h_2(\alpha) \text{ and } \tilde{g}(\tilde{\beta}) = 0$$

it follows that $\tilde{g}(\frac{h_1(\alpha)}{h_2(\alpha)}) = 0$. Let $\hat{g} \in \mathbb{Q}[t, u]$ be a homogeneous polynomial with $\hat{g}(t, 1) = \tilde{g}(t)$. This implies $f = \hat{g}(h_1, h_2)$. □

We remark that the subfield algorithm in [Klüners and Pohst, 1997] calculates the generating polynomial g in a way that we can choose $\tilde{g} = g$ in Lemmas 3.4 and 3.5. Therefore we find a functional or homogeneous bivariate decomposition if it exists.

In general, small coefficients of the generating polynomials of the computed subfields yield decompositions with small coefficients as well. We use the OrderShort function in Kash [Daberkow et al., 1997] which produces a shorter generating polynomial for a number field together with the embedding from one representation to the other. The algorithm is based on the LLL-algorithm [Lenstra et al., 1982] and a slight modification of the algorithm presented in [Cohen, 1993, section 4.4.2].

4. Towers of algebraic number fields

In this section we develop an algorithm which expresses the roots of a polynomial f if we know a tower of subfields of K. We have the following situation: $K = \mathbb{Q}(\alpha)$ is a number field generated by the polynomial f, $L = \mathbb{Q}(\beta)$ is a subfield of K generated by g_1, and $M = \mathbb{Q}(\gamma)$ is a subfield of L generated by g_2 of degree l. In an optimal case we know the embedding polynomials $\omega_1, \omega_2 \in \mathbb{Q}[t]$ with $\omega_1(\alpha) = \beta$ and $\omega_2(\beta) = \gamma$ in which we can express the roots of f in the following way:

Lemma 4.1. *Let $h_1 = \gcd_{L[t]}(f, \omega_1 - \beta)$ and $h_2 = \gcd_{M[t]}(g_1, \omega_2 - \gamma)$. Then we obtain*

$$f = N_{g_1}(h_1) = N_{N_{g_2}(h_2)}(h_1).$$

Proof. In Theorem 3.3 we proved $f = N_{g_1}(h_1)$ and $g_1 = N_{g_2}(h_2)$. The assertion follows immediately. □

In general, we have the following situation: $\mathbb{Q} \subset M = \mathbb{Q}(\gamma) \subset L = \mathbb{Q}(\beta) \subset K = \mathbb{Q}(\alpha)$ and we know the embeddings $\omega_1(\alpha) = \beta$ and $\tau(\alpha) = \gamma$. In order to use the above Lemma we have to calculate the embedding $\omega_2(\beta) = \gamma$.

Lemma 4.2. *Let $\gamma = \sum_{i=0}^{n-1} c_i \alpha^i$ and $\beta^j = \sum_{i=0}^{n-1} b_{i,j} \alpha^i$ $(0 \le j \le m-1)$. Let $B = (b_{i,j})_{\substack{0 \le i \le n-1 \\ 0 \le j \le m-1}}$, $\bar{c} = (c_0, \ldots, c_{n-1})^t$, and $\bar{x} = (x_0, \ldots, x_{m-1})^t$ with $B\bar{x} = \bar{c}$. Then $\gamma = \sum_{j=0}^{m-1} x_j \beta^j$.*

Proof. The system of linear equations has exactly one solution since $\gamma \in \mathbb{Q}(\beta)$. □

After decomposing $f = N_{N_{g_2}(h_2)}(h_1)$ we have two representations for the polynomial $h_2 \in L[t]$. The first one represents the coefficients of h_2 in the basis $1, \beta, \ldots, \beta^{m-1}$. We call this an absolute representation. The other representation uses the basis $\{\gamma^i \beta^j \mid 0 \le i \le l-1, 0 \le j \le \frac{m}{l} - 1\}$. We call this a relative representation. In most cases the relative representation gives a shorter description of the zeros. Our algorithm produces either representation.

5. Examples

We give four examples to demonstrate how efficient this algorithm works. [Hulpke, 1995] gave a list of examples which demonstrates that the other known methods are limited to examples of small degree and small size of coefficients. The first step of most of the other methods is the factorization of polynomials over number fields. We give the computing time (if possible) for this factorization to get an impression how complicate it is to factorize polynomials. All computations were done on a Sun-Ultra-2 300 Mhz using KASH 1.9 under SunOS 5.6.

Let $f(t) = t^8 - 8t^7 + 1448t^6 - 8576t^5 - 203394t^4 + 870600t^3 + 3596804t^2 - 8957592t + 4818366$ which has five decompositions of the form $f = N_{N_g(h_1)}(h_2)$. The computation was done in 0.8 seconds. The corresponding factorization of f over the number field generated by a zero of f took 0.7 seconds. One of these decomposition is:

1. $g(t) = t^2 - 12t + 14$
2. $h_1(t) = t^2 + (-6 + \beta)t + 5$
3. $h_2(t) = t^2 - 2t + (\frac{1}{5}(-1970 + 783\gamma + 625\gamma^2 - 224\gamma^3))$
4. $h_2(t) = t^2 - 2t + ((325 - 224\beta) + (145 - 125\beta)\gamma)$

We remarked in the introduction that the norm decomposition reduces the problem of solvability by radicals to primitive extensions. If the degree of these extensions is not bigger than four it is easy to express the roots by radicals. In our example we use the printed decomposition and get:

$$\beta_{1,2} = 6 + \epsilon_1\sqrt{22} \text{ with } \epsilon_1 = \pm 1.$$

$$\gamma_{j_1,j_2} = 3 - \frac{\beta - \epsilon_2\sqrt{2}}{2} \text{ with } \epsilon_2 = \pm 1, \text{ hence}$$

$$\gamma_{1,2,3,4} = \frac{-\epsilon_1\sqrt{22} + \epsilon_2\sqrt{2}}{2}$$

$$\text{with } \epsilon_1 = \pm 1, \epsilon_2 = \pm 1.$$

$$\alpha_{k_1,k_2} = 1 + \epsilon_3\sqrt{-324 + 224\beta - 145\gamma + 125\beta\gamma} \text{ with } \epsilon_3 = \pm 1, \text{ hence,}$$

$$\alpha_{1,2,3,4,5,6,7,8} =$$

$$1 + \epsilon_3\sqrt{-324+224(6+\epsilon_1\sqrt{22})-145(\frac{-\epsilon_1\sqrt{22}+\epsilon_2\sqrt{2}}{2})+125(6+\epsilon_1\sqrt{22})(\frac{-\epsilon_1\sqrt{22}+\epsilon_2\sqrt{2}}{2})}$$

$$\text{with } \epsilon_1 = \pm 1, \epsilon_2 = \pm 1, \epsilon_3 = \pm 1.$$

Let $f(t) = t^{12} + 9t^{11} + 3t^{10} - 73t^9 - 177t^8 - 267t^7 - 315t^6 - 267t^5 - 177t^4 - 73t^3 + 3t^2 + 9t + 1$ be the polynomial given in [Lazard and Valibouze, 1993]. We compute three inequivalent norm decompositions without any prior knowledge about the polynomial.

After 3.1 seconds we get the following three decompositions of the form $N_{N_g(h_1)}(h_2)$ in an absolute representation (or a relative representation, respectively). The factorization of f over the number field generated by a zero of f took 5.9 seconds. We remark that the "nested" equations in [Lazard and Valibouze, 1993] give a shorter representation of the zeros of f. The main reason is that they choose optimal polynomials for this special example. In the following β and γ denote zeros of g and h_1, respectively. For reasons of space we only give one decomposition.

1. $g(t) = t^2 - 3t - 3$
2. $h_1(t) = t^2 + (-2 + \beta)t + 1$
3. $h_2(t) = t^3 + (6 + 5\gamma - \gamma^2 - \gamma^3)t^2 + (1 + \gamma - 2\gamma^2)t - 1$
4. $h_2(t) = t^3 + ((9 - \beta) + (-3 + 2\beta)\gamma)t^2 + (3 + (-3 + 2\beta)\gamma)t - 1$

Now we consider two larger examples.

$f(t) = t^{32} - 32t^{31} + 496t^{30} - 4888t^{29} + 34340t^{28} - 183880t^{27} + 786400t^{26} - 2779240t^{25} + 8268310t^{24} - 20688072t^{23} + 42882496t^{22} - 72010200t^{21} + 97632348t^{20} - 97228120t^{19} - 33958464t^{18} + 705826648t^{17} - 2475191663t^{16} + 5229698952t^{15} - 7657389040t^{14} + 11103317744t^{13} - 18441575432t^{12} + 23625143936t^{11} - 26861294400t^{10} - 79950368240t^{9} + 226681340832t^{8} - 351779300352t^{7} + 414312426688t^{6} - 379633855232t^{5} + 329006420544t^{4} - 240737112960t^{3} + 154135928576t^{2} - 63365093120t + 18408410368.$

The number field generated by a zero of f has three non-trivial subfields, two of degree 4 and one of degree 16. We computed two decompositions of the form $N_{N_g(h_1)}(h_2)$ in 46 seconds. About 40% of the time was used to find shorter representations for the subfields (OrderShort). The factorization of f over the number field generated by a zero of f was impossible within 3 days. One decomposition is:

1. $g(t) = t^4 + 8t^3 + 24t^2 + 31t + 16$
2. $h_1(t) = t^4 + (-2 - \gamma)t^3 + \gamma$
3. $h_2(t) = t^2 + (\frac{1}{686}(-21732 - 20736\gamma - 15842\gamma^2 - 9583\gamma^3 + 25248\gamma^4 + 24342\gamma^5 + 14805\gamma^6 + 13572\gamma^7 - 10566\gamma^8 - 5565\gamma^9 - 7776\gamma^{10} - 6198\gamma^{11} + 343\gamma^{12} + 1444\gamma^{13} + 1296\gamma^{14} + 1033\gamma^{15}))t + (\frac{1}{196}(17676 + 17416\gamma + 14866\gamma^2 + 9237\gamma^3 - 25336\gamma^4 - 23638\gamma^5 - 14263\gamma^6 - 13804\gamma^7 + 12086\gamma^8 + 5519\gamma^9 + 8144\gamma^{10} + 6642\gamma^{11} - 493\gamma^{12} - 1612\gamma^{13} - 1448\gamma^{14} - 1171\gamma^{15}))$
4. $h_2(t) = t^2 + (\frac{1}{2}((4 + 4\beta) + (-30 - 40\beta - 16\beta^2 - 2\beta^3)\gamma^2 + (23 + 24\beta + 8\beta^2 + \beta^3)\gamma^3))t + (\frac{1}{4}((12 + 12\beta + 4\beta^2) + (-56 - 96\beta - 48\beta^2 - 8\beta^3)\gamma + (34 + 24\beta - 2\beta^3)\gamma^2 + (37 + 56\beta + 24\beta^2 + 3\beta^3)\gamma^3))$

This example demonstrates that the relative representation is much shorter than the absolute one.

The last example I got from Daniel Lazard. The number field given by a zero of f has two non trivial subfields, one of degree 5 and one of degree 8. It took 19 minutes to compute the decompositions. In this example we do not have included the time to find nicer representations. We do not give any output to save space. One problem of our algorithm is to choose a good prime to do the computations. In this examples the chosen prime was not the best one. If we choose the prime by hand we can do the computation within 102 seconds. The factorization of f over the number field generated by a zero of f was impossible within 3 days.

$f(t) = 6436343t^{40} - 34700284t^{39} - 905589810t^{38} + 3408895573t^{37} + 59330876659t^{36} - 114609011287t^{35} - 2146765884442t^{34} + 5816683124493t^{33} + 47966892655022t^{32} + 58086065686110t^{31} - 664273174842926t^{30} - 1793570319828018t^{29} + 4914461478555900t^{28} + 25106824391937532t^{27} - 20936492247511164t^{26} - 173336635271317655t^{25} - 254426897796933790t^{24} + 392882585322815188t^{23} + 178190336390605271 5t^{22} + 230082107372169802 2t^{21} - 304425126707079466 0t^{20} - 194534325710613406 87t^{19} - 202506919175311619 54t^{18} + 552277744485062629 96t^{17} + 135619533598051236796t^{16} - 362202133761690016 13t^{15} - 366983017878149748835t^{14} - 189737074857945494650t^{13} + 514466502292905094369t^{12} + 578377903845523688438t^{11} - 309701724291250465911t^{10} - 734169416313703303879t^{9} - 832705195002762938 78t^{8} + 459451216519714656526t^{7} + 230165980213575319883t^{6} - 112015867904431532196t^{5} - 117712533422275973284t^{4} - 113554461198811893 84t^{3} + 181714768414900037 10t^{2} + 71529809823462260 40t + 811597135529898169$

6. Comparison

The algorithms for computing functional decompositions [Kozen and Landau, 1989] are very efficient in theory and in practice. We want to look at irreducible polynomials in $\mathbb{Q}[t]$ where no functional decomposition exists. We give a concept of decomposition which is the best possible in the sense that to every block system there exists a decomposition. One advantage of our

representation is that we describe the decomposition in an elegant way by an equation ($f = N_g(h)$).

Most of the known algorithms [Landau and Miller, 1985, Hulpke, 1995], and [Lazard and Valibouze, 1993] are based on the factorization of polynomials over number fields resp. the factorization of polynomials of high degree over the rationals. These factorizations are known to be in polynomial time [Landau, 1985, Lenstra et al., 1982]. It is well known that in practice the factorization method based on Hensel's lemma and the recombination procedure is used. This approach is exponential time in the worst case but it works well in practice. Therefore we have a problem where polynomial time algorithms are known but many computed examples show that these algorithms are limited to small examples. We computed a lot of examples up to degree 60 to demonstrate the efficiency of the algorithm. We have a lot of examples where it is possible to compute all decompositions within a minute and it is impossible to factorize the minimal polynomial over the number field within a day. We remark that the algorithm presented in [Casperson et al., 1996] needs no factorization. It is directly based on the lattice reduction [Lenstra et al., 1982]. Practical experiments [Hulpke, 1995, Klüners and Pohst, 1997] show that this method is limited to small examples, too.

The algorithm presented in this paper is mainly based on two steps. First the computation of subfields and second the computation of greatest common divisors of polynomials over number fields (Theorem 3.3). The second step can be done in a very efficient way using modular algorithms presented in [Encarnación, 1995]. We give a short analysis of the used subfield algorithm [Klüners and Pohst, 1997]. Roughly speaking the algorithm can be divided into two parts. First a combinatorical approach is used to find the block systems. Once a block system is known the efficient Hensel lifting resp. Newton lifting procedure is used to determine the corresponding subfield. The latter part of the algorithm is in polynomial time. It may happen in the worst case that exponentially many combinations have to be considered to determine the block systems. The number of combinations is dependent on the degree and the Galois group of the given field. It turns out that we are in the worst case if the Galois group is elementary Abelian. In the Abelian case there is a very efficient algorithm [Acciaro and Klüners, 1998] which computes all automorphisms of the given field. Knowing this it is easy to compute the subfields. Since the number of combinations is not dependent on the size of the coefficients the subfield algorithm is polynomial time in the size of the coefficients.

References

[Acciaro and Klüners, 1998] Acciaro, V. and Klüners, J. (1998). Computing automorphisms of abelian number fields. to appear in Math. Comput.

[Casperson et al., 1996] Casperson, D., Ford, D., and McKay, J. (1996). Ideal decompositions and subfields. *J. Symb. Comput.*, 21:133–137.

[Cohen, 1993] Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Springer.

[Daberkow et al., 1997] Daberkow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K., and Wildanger, K. (1997). KANT V4. *J. Symb. Comput.*, 24(3):267–283.

[Dixon, 1990] Dixon, J. (1990). Computing subfields in algebraic number fields. *J. Austral. Math. Soc. (Series A)*, 49:434–448.

[Encarnación, 1995] Encarnación, M. (1995). Computing GCDs of polynomials over algebraic number fields. *J. Symb. Comput.*, 20:299–313.

[Hulpke, 1995] Hulpke, A. (1995). Block systems of a Galois group. *Exp. Math.*, 4(1):1–9.

[Klüners and Pohst, 1997] Klüners, J. and Pohst, M. (1997). On computing subfields. *J. Symb. Comput.*, 24(3):385–397.

[Kozen and Landau, 1989] Kozen, D. and Landau, S. (1989). Polynomial decomposition algorithms. *J. Symb. Comput.*, 7:445–456.

[Landau, 1985] Landau, S. (1985). Factoring polynomials over algebraic number fields. *SIAM J.Comput.*, 14:184–195.

[Landau and Miller, 1985] Landau, S. and Miller, G. (1985). Solvability by radicals is in polynomial time. *J. of Computer and System Sciences*, 30:179–208.

[Lazard and Valibouze, 1993] Lazard, D. and Valibouze, A. (1993). Computing subfields: Reverse of the primitive element problem. In F. Eyssete, A. G., editor, *MEGA-92, Computational algebraic geometry*, volume 109, pages 163–176. Birkhäuser, Boston.

[Lenstra et al., 1982] Lenstra, A. K., Lenstra Jr., H. W., and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math.Ann.*, 261:515–534.

[von zur Gathen and Weiss, 1995] von zur Gathen, J. and Weiss, J. (1995). Homogeneous bivariate decompositions. *J. Symb. Comput.*, 19:409–434.