Riv. Mat. Univ. Parma (7) **3*** (2004), 233-244

MATHIAS LEDERER (*)

Explicit constructions in splitting fields of polynomials (**)

1 - Introduction

Let K be a field and $f = Z^n + a_1 Z^{n-1} + \ldots + a_n$ a monic univariate polynomial over K. We assume f to be irreducible and separable. Let $x = (x_1, \ldots, x_n)$ be the n-tuple of the zeros of f in some field extension of K, and let $T = (T_1, \ldots, T_n)$ be indeterminates over K. The *relation ideal of f* is the set

$$I = \{P \in K[T];\ P(x) = 0\} \trianglelefteq K[T].$$

Let $L = K(x_1, \ldots, x_n)$ be the splitting field of f. Consider the following easy consequence of the Homomorphism Theorem:

Proposition 1.1. *The mapping* $\phi : K[T]/I \to L : \overline{P} \mapsto P(x)$ *is a K-algebra isomorphism.*

Proposition 1.1 allows us to perform computations in the field L-but only if we know generators of the ideal I. In this case we can perform computations in $K[T]/I$ by using a Gröbner basis of I. However, the definition of I does not automatically lead us to a generating set of I. The situation is even worse – so far no efficient way to compute a system of generators of the relation ideal of a polyno-

---

(*) Institut für Mathematik, Universität Innsbruck, Innsbruck, Austria; e-mail: mathias.lederer@uibk.ac.at

(**) Received March 15th 2004, and in revised form August 4th 2004. AMS classification 12 E 30, 12 F 10, 11 Y 40.

mial was known. The papers [**2**] and [**1**] contain parts of the solution of this problem. The latter paper is based on the following idea: Define K_1 to be the field generated over K by one zero of f. Then factor f over K_1. Take a factor and define an extension $K_2 \mid K_1$ generated over K_1 by a root of it. Now factor f over K_2. Repeat this procedure until f factors completely. Unfortunately this method is not very practical.

We will present a method to construct a Gröbner basis of the relation ideal that is based on the usage of the Galois group of f. Knowing the Galois group including the explicit action on the roots allows one to omit the factorisation. Our crucial result is an interpolation formula for the elements of the Gröbner basis which involves the zeros of f and the Galois group of f, acting on the zeros. Afterwards we will apply our results to a classical theorem of Galois. This theorem states the existence of specific polynomials but gives no hint how to construct the polynomials in practice. We will construct the polynomials in question. Furthermore, we will make use of some p-adic techniques (similar to those of [4]) in order to compute a number of examples over the ground field $\mathbb{Q}$. Finally, we point at a property of the generators that cannot be explained within the theory that was used here.

2 - Generators of the relation ideal

For $i = 1, \ldots, n$, define the field $K_i = K(x_1, \ldots, x_i)$, and set $K_0 = K$. Then clearly $K_i = K_{i-1}(x_i)$ for $i = 1, \ldots, n$, and x_i is a primitive element of the field K_i over the field K_{i-1}. Let f_i be the minimal polynomial of x_i over K_{i-1}. Then $d_i = \deg(f_i)$ is the degree of the field extension $K_i \mid K_{i-1}$. Therefore the polynomial f_i has the shape

$$f_i = T_i^{d_i} + \sum_{k_i=1}^{d_i} b_{i,k_i} T_i^{d_i - k_i},$$

where all coefficients b_{i,k_i} lie in K_{i-1}. The degree of the field extension $K_i \mid K$ equals $d_1 \ldots d_i$. It is easy to see that the family $x_1^{d_1-k_1} \ldots x_{i-1}^{d_{i-1}-k_{i-1}}$, where $1 \leq k_j \leq d_j$ for $j = 1, \ldots, i-1$, is a K-basis of K_{i-1}. Thus the coefficients of the polynomial f_i can uniquely be written as

$$b_{i,k_i} = \sum_{k_1=1}^{d_1} \ldots \sum_{k_{i-1}=1}^{d_{i-1}} b_{i,k_1,\ldots,k_i} x_1^{d_1-k_1} \ldots x_{i-1}^{d_{i-1}-k_{i-1}},$$

all $b_{i, k_1, \dots, k_i}$ belonging to K. (For $i = 1$, no summation has to be done and we simply have $b_{1, k_1} \in K$.) We obtain:

$$f_i = T_i^{n_i} + \sum_{k_1 = 1}^{d_1} \dots \sum_{k_i = 1}^{d_i} b_{i, k_1, \dots, k_i} x_1^{d_1 - k_1} \dots x_{i-1}^{d_{i-1} - k_{i-1}} T_i^{d_i - k_i}. \tag{2.1}$$

Now we define

$$\widehat{f}_i = T_i^{d_i} + \sum_{k_1 = 1}^{d_1} \dots \sum_{k_i = 1}^{d_i} b_{i, k_1, \dots, k_i} T_1^{d_1 - k_1} \dots T_{i-1}^{d_{i-1} - k_{i-1}} T_i^{d_i - k_i}, \tag{2.2}$$

thus $\widehat{f}_i \in K[T_1, \dots, T_i]$. We will use the identity $f_i = \widehat{f}_i(x_1, \dots, x_{i-1}, T_i)$. In what follows all polynomials $\widehat{f}_1, \dots, \widehat{f}_i$ are considered to lie in $K[T_1, \dots, T_i]$.

Theorem 2.1. *The evaluation homomorphism*

$$\phi_i \colon K[T_1, \dots, T_i]/(\widehat{f}_1, \dots, \widehat{f}_i) \to K_i \colon \overline{P} \mapsto P(x_1, \dots, x_i)$$

is a K-algebra isomorphism for $i = 1, \dots, n$. In particular, $I = (\widehat{f}_1, \dots, \widehat{f}_n)$.

Proof. Consider the homomorphism $\psi_i \colon K[T_1, \dots, T_i] \to K(x_1, \dots, x_i)$ defined by $\psi_i(P) = P(x_1, \dots, x_i)$. We have to show that $\ker(\psi_i) = (\widehat{f}_1, \dots, \widehat{f}_i)$. Obviously, $\ker(\psi_i) \supseteq (\widehat{f}_1, \dots, \widehat{f}_i)$. We show the converse inclusion by induction over i.

For $i = 1$, the assertion is well known. For $i > 1$, we will make use of two isomorphisms. The first is $\alpha : K_{i-1}[T_i]/(f_i) \to K_i \colon \overline{P} \mapsto P(x_i)$. For the second, the induction hypothesis says that

$$\phi_{i-1} \colon K[T_1, \dots, T_{i-1}]/(\widehat{f}_1, \dots, \widehat{f_{i-1}}) \to K_{i-1} \colon \overline{P} \mapsto P(x_1, \dots, x_{i-1})$$

is an isomorphism. We adjoin to the domain of definition of ϕ_{i-1} and to the range of ϕ_{i-1} the variable T_i and obtain the second isomorphism,

$$\beta : K[T_1, \dots, T_i]/(\widehat{f}_1, \dots, \widehat{f_{i-1}}) \to K_{i-1} \colon \overline{P} \mapsto P(x_1, \dots, x_{i-1}, T_i).$$

Let $P = P(T_1, \dots, T_i)$ lie in the kernel of ψ_i. In view of α, we conclude that $P(x_1, \dots, x_{i-1}, T_i)$ is a multiple of f_i by a polynomial in $K_{i-1}[T_i]$, so

$$P(x_1, \dots, x_{i-1}, T_i) = Q(x_1, \dots, x_{i-1}, T_i) f_i(T_i),$$

for a suitable $Q \in K[T_1, \dots, T_i]$. In view of β, the equation

$$P(x_1, \dots, x_{i-1}, T_i) - Q(x_1, \dots, x_{i-1}, T_i) f_i(T_i) = 0 ,$$

shows that $P - Q\widehat{f}_i$ lies in the ideal spanned by $\widehat{f}_1, \dots, \widehat{f_{i-1}}$. This shows that P lies in the ideal spanned by $\widehat{f}_1, \dots, \widehat{f}_i$. ■

The polynomial $\widehat{f}_i$ has degree d_i in T_i and is monic in T_i. None of the $T_j, j > i$ occur in $\widehat{f}_i$, and all of the $T_j, j < i$, occur to a power strictly smaller than d_j. From that follows that the $\widehat{f}_i$ form a Gröbner basis with respect to the lexicographical ordering $T_1 < \dots < T_n$.

3 - An interpolation formula for the generators

Now if we are given only the polynomial f, we do not have all the minimal polynomials f_i. Thus we do not have the polynomials $\widehat{f}_i$ either. Now we develop a multivariate interpolation formula in the spirit of Lagrange interpolation which will yield the coefficients of $\widehat{f}_i$. The idea is the following: First think of $\widehat{f}_i$ as a polynomial that lies in $L[T_1, \dots, T_i]$ and prescribe the value of this polynomial at a sufficiently large number of points. Then the interpolation formula establishes the coefficients of $\widehat{f}_i$.

In this Section, we will use the Galois group $G = \mathrm{Gal}(L|K) = \{\sigma_1, \dots, \sigma_N\}$ and, for $i = 1, \dots, n$, its subgroups $G_i = \mathrm{Gal}(L|K_i)$. By definition of K_i, we have $G_i = \{\sigma \in G; \sigma(x_j) = x_j, j \leq i\}$.

Lemma 3.1. *Let $L|K$ and G be as above. For $y \in L$, set $Gy = (\sigma_1(y), \dots, \sigma_N(y)) \in L^N$ Then for arbitrary $y_1, \dots, y_r \in L$, the following statements are equivalent*:

(i) *$y_1, \dots, y_r \in L$ are K-linearly independent.*

(ii) *$Gy_1, \dots, Gy_r \in L^N$ are L-linearly independent.*

Proof. We point out that this lemma is quite similar to Artin's Lemma and only give a proof of the nontrivial direction $(i) \Rightarrow (ii)$. Assume that $y_1, \dots, y_r$ are K-linearly independent but $Gy_1, \dots, Gy_k$ (where $k < r$) form an L-basis of ${}_L\langle Gy_1, \dots, Gy_r\rangle$. Then there exist uniquely determined coefficients $\lambda_1, \dots, \lambda_r \in L$ satisfying $Gy_{k+1} = \sum_{i=1}^{k} \lambda_i Gy_i$. For every $\sigma \in G$, there exists a matrix $P \in GL_N(K)$ satisfying $\sigma(Gy) = PGy$ for all $y \in L$. We obtain $PGy_{k+1} = \sigma(y_{k+1}) = \sum_{i=1}^{k} \sigma(\lambda_i)\, \sigma(Gy_i) = \sum_{i=1}^{k} \sigma(\lambda_i)\, PGy_i = P \sum_{i=1}^{k} \sigma(\lambda_i)\, Gy_i$ and there from $Gy_{k+1} = \sum_{i=1}^{k} \sigma(\lambda_i)\, Gy_i$. Since $Gy_1, \dots, Gy_k$ is a basis of ${}_L\langle Gy_1, \dots, Gy_r\rangle$, Gy_{k+1} is uniquely written as an L-linear combination of these vectors, and therefore $\sigma(\lambda_i) = \lambda_i$ for $i = 1, \dots, k$ and for all $\sigma \in G$. Since $K = \mathrm{Fix}(G)$, the coefficient λ_i must lie in K for all $i = 1, \dots, k$. Thus also y_{k+1} lies in ${}_K\langle y_1, \dots, y_r \rangle$, a contradiction to the K-linear independence of $y_1, \dots, y_r$. ■

Proposition 3.1. *$L[T_1, \dots, T_i]$ contains exactly one polynomial of the shape* (2.2) *vanishing at $(\sigma(x_1), \dots, \sigma(x_i))$ for all $\sigma \in G$. The coefficients of this polynomial lie in K.*

Proof. First we note that $\widehat{f}_i$ has the desired property: $f_i(x_i) = \widehat{f}_i(x_1, \dots, x_i) = 0$, and also $\sigma(\widehat{f}_i(x_1, \dots, x_i)) = \widehat{f}_i(\sigma(x_1), \dots, \sigma(x_i)) = 0$ for all $\sigma \in G$. This proves the existence as claimed in the proposition. Of course, the coefficients of $\widehat{f}_i$ lie in K.

Since the family $x_1^{d_1 - k_1} \dots x_i^{d_i - k_i}$, where $1 \leqslant k_j \leqslant d_j$ for $j = 1, \dots, i$, is a K-basis of K_i, Lemma 3.1 implies that the family $(Gx_1^{d_1 - k_1} \dots x_i^{d_i - k_i})$, where $1 \leqslant k_j \leqslant d_j$ for $j = 1, \dots, i$, is L-linearly independent. Thus the coefficients $b_{i, k_1, \dots, k_i} \in L$ in the sum

$$-Gx_i^{d_i} = \sum_{k_1 = 1}^{d_1} \dots \sum_{k_i = 1}^{d_i} b_{i, k_1, \dots, k_i} Gx_1^{d_1 - k_1} \dots x_i^{d_i - k_i}$$

are uniquely determined. In other words, the coefficients of a polynomial having the shape (2.2) are uniquely determined under the assumption that the polynomial vanishes at $(\sigma(x_1), \dots, \sigma(x_i))$ for all $\sigma \in G$. This proves the uniqueness as claimed in the proposition. ■

For the interpolation we will need the following sets: For $\varrho \in G$ and $i = 1, \dots, n$, define $B^{(\varrho, i)} = \{\sigma(x_i);\ \sigma \in G,\ \sigma|_{K_{i-1}} = \varrho|_{K_{i-1}}\} \setminus \{\varrho(x_i)\}$. Thus $B^{(\varrho, i)}$ consists of the translates $\sigma(x_i)$, where σ runs through all extensions of $\varrho|_{K_{i-1}}$ to K_i, minus the element $\varrho(x_i)$.

Lemma 3.2. $|B^{(\varrho, i)}| = d_i - 1$ for all $\varrho \in G$ and for all $i \in \{1, \dots, n\}$.

Proof. The number of extensions σ of $\varrho|_{K_{i-1}}$ to K_i equals the degree of the field extension $K_i | K_{i-1}$, i.e. d_i. Two extensions of this kind are different if and only if they take different values $\sigma(x_i)$, since x_i generates K_i over K_{i-1}. ■

Theorem 3.3. *The i-th generating polynomial $\widehat{f}_i$ of the relation ideal I is given by*

$$\widehat{f}_i = T_i^{d_i} - \sum_{\varrho \in G//G_i} \varrho(x_i)^{d_i} \prod_{y_1 \in B^{(\varrho, 1)}} \frac{T_1 - y_1}{\varrho(x_1) - y_1} \dots \prod_{y_i \in B^{(\varrho, i)}} \frac{T_i - y_i}{\varrho(x_i) - y_i}, \tag{3.1}$$

where $G//G_i$ is a system of representatives of the cosets G/G_i, $i = 1 \dots, n$.

Proof. We define g by the right hand side of (3.1) and prove $\widehat{f}_i = g$. Lemma 3.2 shows that $\deg_j(g) \leq d_j - 1$, for $j = 1, \dots, i-1$. Clearly $\deg_i(g) = d_i$. Thus the multidegree of g has the properties that we demanded for $\widehat{f}_i$. If we can prove that $g(\sigma(x_1), \dots, \sigma(x_i)) = 0$ for all $\sigma \in G$, it will follow from Proposition 3.1 that $\widehat{f}_i$ and g coincide.

So let $\sigma \in G$ be given. Take $\varrho' \in G//G_i$ such that $\sigma = \varrho' \tau$, for a suitable $\tau \in G_i$. In particular, for $j = 1, \dots, i$ we have $\sigma(x_j) = \varrho' \tau(x_j) = \varrho'(x_j)$ since $\tau(x_j) = x_j$. In order to show that $g(\sigma(x_1), \dots, \sigma(x_i)) = 0$, we focus our attention on the sum $\sum_{\varrho \in G//G_i}$. The automorphisms ϱ occurring as summation index belong to the two categories $\varrho = \varrho'$ and $\varrho \neq \varrho'$. If $\varrho = \varrho'$, the respective summand of becomes $\sigma(x_i)^{d_i}$ for in this case $\sigma(x_j) = \varrho'(x_j) = \varrho(x_j)$, hence $(\sigma(x_j) - y_j)/(\varrho(x_j) - y_j) = 1$ for all $j = 1, \dots, i$. In the case $\varrho \neq \varrho'$ we can find a number $j \in \{1, \dots, i\}$ satisfying $\varrho(x_j) \neq \varrho'(x_j)$. Thus $\varrho'(x_j)$ lies in $B^{(\varrho, j)}$, and therefore there is a $y_j \in B^{(\varrho, j)}$ such that $y_j = \varrho'(x_j) = \sigma(x_j)$. The summand corresponding to this ϱ vanishes, since the product occurring in in the sum contains the factor $\sigma(x_j) - y_j$ where $y_j = \varrho'(x_j) = \sigma(x_1)$. Altogether, we obtain $g(\sigma(x_1), \dots, \sigma(x_i)) = \sigma(x_i)^{d_i} - \sigma(x_i)^{d_i} = 0$. ∎

4 - On a theorem of Galois

The following theorem is due to E. Galois (for the proof see e.g. [5]):

Theorem 4.1 (Galois). *Let $f \in \mathbb{Q}[Z]$ be an irreducible polynomial of degree p, where p is a prime number. Let L be the splitting field of f and $x_1, \dots, x_p$ the zeros of f in L. Then the following statements are equivalent:*

(i) *f is solvable by radicals.*

(ii) *$L = \mathbb{Q}(x_i, x_j)$ for all $i, j \in \{1, \dots, p\}$ such that $i \neq j$.*

We would like to apply the results of Sections 2 and 3 in order to give an explicit formula for the polynomial dependence of x_k from x_i and x_j. By the theorem, any other zero x_k lies in $\mathbb{Q}(x_i, x_j)$. We choose a numbering of the zeros such that $x_i = x_1$, $x_j = x_2$, $x_k = x_3$. We determine the minimal polynomial $\widehat{f}_3$ of x_3 over K_2. It has degree 1, thus can be written $\widehat{f}_3 = T_3 - P(x_1, x_2)$ for a suitable $P \in K[T_1, T_2]$. We evaluate $\widehat{f}_3$ at x_3 and obtain an equation $x_3 = P(x_1, x_2)$. This is the rational polynomial in two zeros whose existence is claimed in the theorem. Recalling the precise form of $\widehat{f}_3$ in 3.12, we obtain

$$x_3 = \sum_{\varrho \in G//G_3} \varrho(x_3) \prod_{y_1 \in B^{(\varrho, 1)}} \frac{x_1 - y_1}{\varrho(x_1) - y_1} \prod_{y_2 \in B^{(\varrho, 2)}} \frac{x_2 - y_2}{\varrho(x_2) - y_2} \, .$$

Note that a priori it is not clear that the right hand side of this formula is a rational polynomial in x_1 and x_2!

5 - Numerical computation of the generators

In this Section we assume $K = \mathbb{Q}$. We will work with complex and p-adic approximations of the zeros of f in order to construct the generators of the relation ideal. This task requires the knowledge of an integer Γ_i such that $\Gamma_i \widehat{f}_i$ has integer coefficients (Proposition 5.1). Further, we need an upper bound for the absolute values of these coefficients (Proposition 5.2). The final result is formulated in Proposition 5.3.

Let γ be a rational integer such that all the products γx_j, $j = 1, \dots, n$, are algebraic integers. We denote the discriminant of f by

$$d(f) = \prod_{1 \leq r < s \leq n} (x_r - x_s)^2 \, .$$

The ceiling function is always denoted by $\lceil \; \rceil$ and the floor function by $\lfloor \; \rfloor$.

Proposition 5.1. *For $i = 1, \dots, n$, the rational integer*

$$\Gamma_i = \gamma^{n(n-1) \lceil \frac{i}{2} \rceil + d_i} d(f)^{\lceil \frac{i}{2} \rceil}$$

has the property that $\Gamma_i \widehat{f}_i$ lies in $\mathbb{Z}[T_1, \dots, T_i]$.

Proof. Recall the interpolation formula (3.1) which we proved in Section 3. We multiply this equation by Γ_i. The factors of $d(f)^{\lceil \frac{i}{2} \rceil}$ cancel down with the denominators $(\varrho(x_j) - y_j)$, and $\gamma^{n(n-1) \lceil \frac{i}{2} \rceil + d_i}$ is needed to make the remaining factors lie in $\mathcal{O}_L[T]$. Thus the coefficients of $\Gamma_i \widehat{f}_i$ lie in $\mathcal{O}_L$ and in $\mathbb{Q}$, that is, in $\mathbb{Z}$. ■

For the time being, let $x_1, \dots, x_n \in \mathbb{C}$ denote the complex zeros of f and $| \; |$ denote the usual absolute value in $\mathbb{C}$.

Proposition 5.2. *Let* $D, M \in \mathbb{R}_{>0}$ *be such that* $M > \max\{|x_r|\}$ *and* $D > \max\{|x_r - x_s|; x_r \neq x_s\}$. *Then the absolute value of* $\Gamma_i b_{i, k_1, \ldots, k_i}$ *is bounded by*

$$\gamma^{n(n-1)\lceil \frac{i}{2}\rceil + d_i} \binom{d_1 - 1}{k_1 - 1} \cdots \binom{d_i - 1}{k_i - 1} M^{k_1 + \ldots + k_i - i + d_i} D^{n(n-1)\lceil \frac{i}{2}\rceil - d_i - \ldots - d_i + i}. \tag{5.1}$$

Proof. We evaluate the formula (3.1) for $\widehat{f}_i$ at the complex zeros and multiply the result by Γ_i. As in the proof of Proposition 5.1 we cancel the denominators $(\varrho(x_j) - y_j)$ by factors of $d(f)^{\lceil \frac{i}{2}\rceil}$. In the remaining product we have $n(n-1)\left\lceil \frac{i}{2}\right\rceil - d_1 - \ldots - d_i + i$ factors of the type $(\xi_r - \xi_s)$ left. The absolute value of these is bounded by D. Further, M is an upper bound for $\varrho(\xi_i)$. Finally, it is easy to check that for $j = 1, \ldots, i$, the absolute value of the coefficient of the polynomial $\prod_{y_j \in B^{(\varrho, j)}} (T_j - y_j)$ at $T_j^{d_j - k_j}$ is bounded by $\binom{d_j - 1}{k_j - 1} M^{k_j - 1}$. Collecting factors, we obtain the result. ■

We fix an integer c such that cf lies in $\mathbb{Z}[Z]$. Let p be a prime number such that the polynomial $\overline{cf} \in (\mathbb{Z}/p\mathbb{Z})[Z]$ (the reduction of cf modulo p) splits into $n = \deg(f)$ disjoint linear factors over $\mathbb{Z}/p\mathbb{Z}$. (The existence of such a prime follows from Chebotarev's density theorem, see e.g. [7].) By Hensel's Lemma, we can lift these zeros to zeros of cf in $\mathbb{Q}_p$. The polynomial cf also splits into n disjoint linear factors over $\mathbb{Z}/p^e\mathbb{Z}$, for all integers $e \leqslant 1$. In this process, if $e < k$, the zeros in $\mathbb{Z}/p^e\mathbb{Z}$ are obtained from the zeros in $\mathbb{Z}/p^k\mathbb{Z}$ by reduction modulo p^e. We call the zeros in $\mathbb{Z}/p^e\mathbb{Z}$ the eth p-adic approximations of the zeros.

For the forthcoming discussion, we let G operate on the p-adic approximations of the zeros in the obvious way. We will need p-adic approximations of $d(f)$, $B^{(\varrho, i)}$, $\widehat{f}_i$ and Γ_i. The approximations are defined by the same formulas as the original objects, but with each zero replaced by the respective approximation. Now we can specify exponents e_i such that from the knowledge of e_ith p-adic approximations of the zeros of f we can compute $\widehat{f}_i$.

Proposition 5.3. *For* $i = 1, \ldots, n$ *the following holds: Let* λ_i *be the maximum of* $|\Gamma_i|$ *and the products* (5.1), *for all* $k_j = 1, \ldots, d_j$. *Define* $e_i = \left\lfloor \frac{\log(2\lambda_i - 1)}{\log(p)} \right\rfloor + 1$. *We view the* e_i*th* p*-adic approximation of* $\Gamma_i \widehat{f}_i$ *as a polynomial in* $\mathbb{Z}[T_1, \ldots, T_i]$ *by using the system of representatives*

$\left\{-\frac{p^{e_i}-1}{2}, \ldots, \frac{p^{e_i}-1}{2}\right\}$ *of* $\mathbb{Z}/p^{e_i}\mathbb{Z}$. *Then this polynomial coincides with* $\Gamma_i \widehat{f}_i$.

Proof. Let $\beta_{i, k_1, \ldots, k_i} \in \left\{-\frac{p^{e_i}-1}{2}, \ldots, \frac{p^{e_i}-1}{2}\right\}$ be the coefficients of the approximate $\Gamma_i \widehat{f}_i$. Then we can find $\mu_{i, k_1, \ldots, k_i} \in \mathbb{Z}$ such that $b_{i, k_1, \ldots, k_i} = \beta_{i, k_1, \ldots, k_i} + \mu_{i, k_1, \ldots, k_i} p^{e_i}$. Now if $\mu_{i, k_1, \ldots, k_i}$ were not zero, we would have $|b_{i, k_1, \ldots, k_i}| \geqslant (p^{e_i}+1)/2$. On the other, hand by definition of e_i we have $e_i > \log(2\lambda_i - 1)/\log(p)$ from which we deduce $\lambda_i < (p^{e_i}+1)/2$. We assumed $|b_{i, k_1, \ldots, k_i}| < \lambda_i$, hence $|b_{i, k_1, \ldots, k_i}| < (p^{e_i}+1)/2$, a contradiction. Thus $\mu_{i, k_1, \ldots, k_i} = 0$ and the proposition is proved. ■

6 - Examples

In this Section we present some examples treated with the methods developed in Section 5. We have used KANT for all computations. This computer algebra system can compute the Galois group of irreducible polynomials of degree $\leqslant 23$ over $\mathbb{Q}$. Meanwhile, KANT also features a function that computes the action of the Galois group on the zeros of f – of course only approximations to the zeros, optionally complex or p-adic.

For various irreducible separable polynomials over $\mathbb{Q}$, we give the following data: The Galois group (by the name it bears in KANT and by generators), the indices $d_1, \ldots, d_n$, the discriminant $d(f)$, a prime p as in Section 5, the exponent e (for KANT reasons a power of 2) up to which the approximate zeros were lifted, the zeros x in $\mathbb{Z}/p\mathbb{Z}$, the generators $\widehat{f}_i$, $i = 2, \ldots, n$ of the relation ideal (note that $\widehat{f}_1 = f$, so we need not include $\widehat{f}_1$ in the list) and the running time of the algorithm. The sample polynomials f were taken from [8]; the same polynomials can be found in [3] or in the database http://www.mathematik.uni-kassel.de/~klueners/minimum/minimum.html by Jürgen Klüners and Gunter Malle. All computations were done on a 333 MHz Ultra 10 Sun SPARC processor running under Solaris 7.

Example 1. ($D(5)$) Running time 0.88 s

$$f = Z^5 - 5Z + 12,\ G = D(5) = \langle (1, 2, 4, 5, 3), (2, 3)(4, 5) \rangle,$$

$$d(f) = 64000000,\ p = 127,\ x = (108, 62, 46, 34, 4),$$

$$\widehat{f}_2 = T_2^2 - 1/4\, T_1^4 T_2 - 1/4\, T_1^3 T_2 - 1/4\, T_1^2 T_2 + 3/4\, T_1 T_2 + T_2 - 1/4\, T_1^4 - 1/4\, T_1^3 - 1/4\, T_1^2 - 5/4\, T_1 + 2,$$

$$\widehat{f}_3 = T_3 + T_2 - 1/4\,T_1^4 - 1/4\,T_1^3 - 1/4\,T_1^2 + 3/4\,T_1 + 1,$$

$$\widehat{f}_4 = T_4 - 1/8\,T_1^4 T_2 + 1/8\,T_1^3 T_2 - 1/8\,T_1^2 T_2 + 1/8\,T_1 T_2 + 1/2\,T_2 \\ + 1/8\,T_1^4 - 1/8\,T_1^3 + 1/8\,T_1^2 - 1/8\,T_1 + 1/2,$$

$$\widehat{f}_5 = T_5 + 1/8\,T_1^4 T_2 - 1/8\,T_1^3 T_2 + 1/8\,T_1^2 T_2 - 1/8\,T_1 T_2 - 1/2\,T_2 \\ 1/8\,T_1^4 + 3/8\,T_1^3 + 1/8\,T_1^2 + 3/8\,T_1 - 3/2\,.$$

Example 2 ($F_{36}(6)$: 2). Running time 29 s

$f = Z^6 + 2Z^4 + 2Z^3 + Z^2 + 2Z + 2$, $G = F_{36}(6)\colon 2 = \langle (1, 2, 5), (1, 3)(2, 4)(5, 6), (1, 4, 2, 3)(5, 6)\rangle$, $d(f) = -187648$, $p = 509$, $x = (456, 339, 252, 226, 223, 31)$,

$$\widehat{f}_2 = T_2^2 + T_1 T_2 + T_1^2 + 1, \widehat{f}_3 = T_3^3 + T_3 + T_1^3 + T_1 + 2,$$

$$\widehat{f}_4 = T_4^2 + T_3 T_4 + T_3^2 + 1, \widehat{f}_5 = T_5 + T_2 + T_1, \widehat{f}_6 = T_6 + T_4 + T_3\,.$$

Example 3 ($C(7)$). Running time 12 s

$$f = Z^7 + Z^6 - 12Z^5 - 7Z^4 + 28Z^3 + 14Z^2 - 9Z + 1, G = C(7) = \langle (1,2,5,3,4,6,7)\rangle,$$

$$d(f) = 171903939769,\ p = 41,\ x = (122, 120, 107, 15, 11, 6, 2),$$

$$\widehat{f}_2 = T_2 - 18/17T_1^6 - 15/17T_1^5 + 210/17T_1^4 + 91/17T_1^3 - 420/17T_1^2 - 216/17T_1 + 45/17,$$

$$\widehat{f}_3 = T_3 - 30/17T_1^6 - 42/17T_1^5 + 350/17T_1^4 + 350/17T_1^3 - 785/17T_1^2 - 700/17T_1 + 160/17,$$

$$\widehat{f}_4 = T_4 + 38/17T_1^6 + 43/17T_1^5 - 449/17T_1^4 - 330/17T_1^3 + 1000/17T_1^2 + 711/17T_1 - 197/17,$$

$$\widehat{f}_5 = T_5 + 27/17T_1^6 + 31/17T_1^5 - 315/17T_1^4 - 230/17T_1^3 + 681/17T_1^2 + 460/17T_1 - 127/17,$$

$$\widehat{f}_6 = T_6 + 15/17T_1^6 + 21/17T_1^5 - 175/17T_1^4 - 175/17T_1^3 + 384/17T_1^2 + 350/17T_1 - 46/17,$$

$$\widehat{f}_7 = T_7 - 32/17T_1^6 - 38/17T_1^5 + 379/17T_1^4 + 294/17T_1^3 - 860/17T_1^2 - 588/17T_1 + 182/17\,.$$

7 - A question

In Section 5, at a certain point we multiplied $\widehat{f}_i$ by the factor Γ_i (essentially a power of the discriminant) in order to obtain a polynomial with coefficients in $\mathbb{Z}$.

Therefore, as for the rational polynomial $\hat{f}_i$, one would expect that the denominators that occur in its coefficients are in the magnitude of Γ_i. But in all examples computed so far, the denominators are significantly smaller than Γ_i. This phenomenon can be explained by a very elementary argument in the case when f has degree n and $G = S_n$, see [**6**]. For the general case this seems to be a more difficult question.

8 - Acknowledgements

I would like to thank Herwig Hauser for awakening my interest in the relation ideal and Kurt Girstmair for telling me what this ideal is good for and for his help during my work on this paper. I would like to thank Alexander Ostermann for his help on interpolation of all kinds and Jürgen Klüners for his help in KANT questions. Thanks to François Brunault for many very useful comments on the text!

References

[1] H. Anai, M. Noro and K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., **143**, 29-50. Birkhäuser, Basel 1996.

[2] Philippe Aubry and Annick Valibouze, *Using Galois ideals for computing relative resolvents*, J. Symbolic Comput. **30** (6) (2000), 635-651.

[3] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin 1993.

[4] Katharina Geissler and Jürgen Klüners, *Galois group computation for rational polynomials* J. Symbolic Comput. **30** (6) (2000), 653-674.

[5] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin 1967.

[**6**] Mathias Lederer, *Explizite Konstruktionen in Zerfällungskörpern von Polynomen*, Master's thesis, Universität Innsbruck 2002.

[7] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **322**, Springer-Verlag, Berlin 1999.

[8] Leonard Soicher, *The computation of Galois groups*, Master's thesis, Concordia University, Montreal 1981.

Abstract

We construct a Gröbner Basis of the relation ideal of a polynomial and give an interpolation formula for the basis elements which is sufficiently explicit to be used in practical computations. We prove a constructive version of a theorem of Galois, concerning the solvability of rational polynomials of prime degree. For a number of example polynomials, the computations are carried out.

* * *