ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 617–636

JOURNAL OF
PURE AND
APPLIED ALGEBRA

A modular method for computing the Galois groups of polynomials

K. Yokoyama

*HPC Research Center, Fujitsu Labs., 1-1 Kamikodanaka y-chome, Nakahara-ku,
Kawasaki 211-88, Japan*

Abstract

We propose a new method to compute the Galois group of an integral polynomial based on resolvent computation by modular techniques. We developed an exact method to find integral roots of relative resolvents by direct evaluation of invariants over some p-adic number field or its extension. Experiments on a set of test polynomials suggest that the presented method is quite practical by virtue of efficient evaluation of invariants based on modular techniques introduced here. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 11R32

1. Introduction

Finding an efficient deterministic algorithm for computing the Galois group of an integral polynomial is a very classical problem. One can find many papers on this problem. In [2] the author, together with colleagues, proposed a method based on computation of the splitting field of a given polynomial. Although it works well for small Galois groups, due to the difficulty of factorization over successive extension fields, it tends to be hard to deal with large Galois groups. In order to deal with polynomials having a large Galois group, it is strongly suggested to use a certain knowledge about the classification of all subgroups in the full symmetric groups. One of the most promising ways is the *use of resolvents*. In a numerical approach, Stauduhar [23] proposed a method based on resolvents (see its continuation [11]). As for a symbolical approach, several authors [3, 22, 25] proposed methods based on absolute resolvents, where absolute resolvents are computed through resultants or symmetric functions. (By making special tables, McKay and his colleagues gave a practical implementation in Maple for polynomials with degrees less than 8 and Arnaudiès and Valibouze also gave practical methods for polynomials up to degree 11. See also [17].) Recently,

PII S0022-4049(97)00030-3

Colin [9] proposed a method based on relative resolvents, which can be viewed a *symbolic* counterpart of Stauduhar's method.

Aiming at a practical deterministic method for computing Galois groups, we apply modular techniques to Stauduhar's method. From a computational view point, the most crucial problem in existing methods based on resolvents is the difficulty of finding a rational integral root of the resolvent for a given subgroup and its invariant. There are two different approaches, numerical and symbolic. In a numerical approach, we compute all roots of a given polynomial numerically and evaluate invariants by approximation. As pointed out in [12], there is a very critical problem: the swell of the required precision for the results in this approach to be reliable. In a symbolic approach, we compute resolvents by resultants or symmetric functions. However, it is very hard to compute absolute resolvents when the target subgroup has large index in the symmetric group. It is also hard to compute relative resolvents, since we have to compute resolvents over algebraic extensions.

In our method, we find integral roots of resolvents by direct evaluation of invariants over some p-adic number field $\boldsymbol{Q}_p$ or an extension, so that we avoid heavy computation of resolvents. Moreover, in this computation, we deal only with invariants appearing in relative resolvents. By precise analysis of the relation between the splitting field of a polynomial f over the field $\boldsymbol{Q}$ of rational numbers and that over $\boldsymbol{Q}_p$, we find a bound k, computable from f, such that we can replace the expressions of roots of f over $\boldsymbol{Q}_p$ or an extension, with their approximations modulo p^{k+1}. Since computation of splitting fields over finite fields is much easier than that over $\boldsymbol{Q}$ and since we can lift splitting fields over $GF(p)$ to those over $\boldsymbol{Q}_p$ modulo p^{k+1} for any integer k efficiently, we can apply modular techniques for efficient evaluation of invariants. We note that Darmon and Ford [10] had already applied the technique *direct evaluation* of the roots by their p-adic approximation in $\boldsymbol{Q}_p$ to prove that two polynomials constructed by some combinatorial objects have M_{11} and M_{12} as their Galois groups. The method here is obtained independently to their work and it gives not only a general formulation, i.e., an algorithm for general polynomials, but also a further improvement, i.e., use of extension fields of p-adic number fields.

In this paper, we also give a discussion to make the method very practical, and report on a computational experiment for polynomials of small degree which suggests the quality and ability of the new method. As for the part of group computation, we rely only on existing works in the field of computational group theory (cf. [7]). The new method provides a *byproduct* which can be immediately applied to compute the splitting field of a polynomial.

2. Mathematical fundamentals

In this section we provide the necessary notions. First we argue over an arbitrary field $\mathscr{Q}$ which is of characteristic 0 or a finite field. Since our goal is to obtain the Galois group, we can assume square-freeness of the polynomials studied.

Let $f(x)$ be a monic square-free polynomial of degree n over $\mathscr{Q}$ and $\Omega_f = \{\alpha_1,\ldots,\alpha_n\}$ the set of all roots of f in the algebraic closure of $\mathscr{Q}$. The splitting field K_f of f is the extension field $\mathscr{Q}(\Omega_f)$ obtained by adjoining all roots to $\mathscr{Q}$. The Galois group G_f of $f(x)$ is the $\mathscr{Q}$-algebra automorphism group of K_f. Since G_f acts faithfully on Ω_f, we treat G_f as its permutation representation on Ω_f.

To express the splitting field K_f symbolically, we set the following: we assign each root α_i to an indeterminate x_i for $i=1,\ldots,n$. For simplicity, we write $X=\{x_1,\ldots,x_n\}$. Then K_f is represented by the residue class ring $\mathscr{A}$ of the polynomial ring $\mathscr{Q}[X]$ factored by the kernel $\mathscr{M}$ of a ring-epimorphism ϕ from $\mathscr{Q}[X]$ to K_f which transforms $g(x_1,\ldots,x_n)$ to $g(\alpha_1,\ldots,\alpha_n)$ for each g in $\mathscr{Q}[X]$. We call the maximal ideal *$\mathscr{M}$ the splitting ideal of f associated with the assignment of the roots* $\alpha_1,\ldots,\alpha_n$. (In [3], they call *$\mathscr{M}$ the ideal of the relations between the roots of f.*) In this setting, to compute the splitting field K_f means to compute a *basis* of $\mathscr{M}$. As we need a unique expression for each element, the required basis must be a Gröbner basis (cf. [4]).

We consider the Galois group G_f as a subgroup of S_n, where S_n acts naturally on $\mathscr{Q}[X]$ with $x_i^\sigma = x_{i^\sigma}$ for $1 \le i \le n$ and $\sigma \in S_n$. Of course, G_f is $\mathrm{Aut}_{\mathscr{Q}}(\mathscr{A})$, the $\mathscr{Q}$-ring automorphism group of $\mathscr{A}$.

Remark 1. Let $\mathscr{G}$ be a Gröbner basis of $\mathscr{M}$. Since $\phi(\mathscr{M})=\{0\}$, $\phi(P)=\phi(\mathrm{NF}_{\mathscr{G}}(P))$ for every P in $\mathscr{Q}[X]$ and especially, $\phi(P)=\mathrm{NF}_{\mathscr{G}}(P)$ if $\phi(P)$ belongs to $\mathscr{Q}$, where $\mathrm{NF}_{\mathscr{G}}(P)$ denotes the normal form of P with respect to $\mathscr{G}$.

Remark 2. Choose the lexicographic order $<$ on terms with $x_1 < \cdots < x_n$. Then the reduced Gröbner basis $\mathscr{G}$ of $\mathscr{M}$ coincides with the generating set $\{g_1,g_2,\ldots,g_n\}$ obtained by *successive extensions* such that for each i,

(1) g_i is a polynomial in $x_1,\ldots,x_i$ and monic with respect to x_i, and

(2) $\mathscr{Q}(\alpha_1,\ldots,\alpha_i) \cong \mathscr{Q}[x_1,\ldots,x_i]/Id(g_1,\ldots,g_i)$, where $Id(F)$ denotes the ideal generated by an element or a set F. This implies that g_i is an irreducible factor of $f(x_i)$ over $\mathscr{Q}[x_1,\ldots,x_{i-1}]/Id(g_1,\ldots,g_{i-1})$ such that $g_i(\alpha_1,\ldots,\alpha_i)=0$.

From this fact, $\mathscr{G}$ can be obtained by "algebraic factoring methods," see [24, 2].

We use the following notation for groups: for a group G acting on a set $\mathscr{S}$, we denote by $\mathrm{Stab}_G(A)$ the stabilizer in G of an element or a subset A of $\mathscr{S}$, i.e., $\mathrm{Stab}_G(A)=\{\sigma\in G \mid A^\sigma = A\}$. If G is the full symmetric group on $\mathscr{S}$, we simply write $\mathrm{Stab}(A)$ for $\mathrm{Stab}_G(A)$. By $H\backslash G$ and $H\backslash\backslash G$ we denote the set of right cosets of H in G and the set of all representatives of $H\backslash G$, respectively.

Now, we introduce the notion of *splitting rings* and of *resolvents*. Then we give several relations on idempotents of splitting rings and resolvents. Here, we use a slightly different terminology from those used in [3, 21].

Definition 3. We call the ideal generated by $s_1+f_1,\ldots,s_n+(-1)^{n-1}f_n$ the *universal splitting ideal* of f and denote it by $\mathscr{M}_0$, where s_i is the ith elementary symmetric function on X and $f(x)=x^n+f_1x^{n-1}+\cdots+f_n$. We call the residue class ring $\mathcal{Q}[X]/\mathcal{M}_0$ the *universal splitting ring of* f over $\mathcal{Q}$ and denote it by $\mathcal{A}_0$. Moreover, we call the following set the *standard generating set* of $\mathcal{M}_0$:

$$\{g_1(x_1), g_2(x_1,x_2), \ldots, g_n(x_1,\ldots,x_n)\},$$

where $g_1(x_1)=f(x_1)$ and $g_i(x_1,\ldots,x_i)$ is the quotient of $f(x_i)$ divided by $((x_i-x_1)\cdots(x_i-x_{i-1}))$ for each $i>1$. The standard generating set is the reduced Gröbner basis of $\mathcal{M}_0$ with respect to the lexicographic order $<$ on terms such that $x_1<\cdots<x_n$. The universal splitting ideals and the universal splitting rings can be defined over rings.

Usually, for each polynomial g in $\mathcal{Q}[X]$, we express the residue class containing g by the normal form of g with respect to the standard generating set. However, we sometimes express the residue class by g.

Since S_n stabilizes $\mathcal{M}_0$, S_n also acts faithfully on $\mathcal{A}_0$, i.e., $S_n\subset \mathrm{Aut}_{\mathcal{Q}}(\mathcal{A}_0)$. As f is square-free, we have the following.

Theorem 4 (Pohst and Zassenhaus [21]). *The universal splitting ring $\mathcal{A}_0$ has finitely many primitive idempotents $e_1,\ldots,e_\ell$ such that $\{e_1,\ldots,e_\ell\}$ forms an S_n-orbit. Therefore,* $\mathrm{Stab}(e_1),\ldots,\mathrm{Stab}(e_\ell)$ *are pairwise isomorphic and the number ℓ of primitive idempotents coincides with* $[S_n:\mathrm{Stab}(e_1)]$. *Moreover, for each i, $e_i\mathcal{A}_0\cong K_f$ and* $\mathrm{Aut}_{\mathcal{Q}}(e_i\mathcal{A}_0)=\mathrm{Stab}(e_i)$.

By [3, p. 17], we have $\mathcal{M}_0=\bigcap_{\sigma\in G_f\backslash\backslash S_n}\mathcal{M}^\sigma$ and for each σ in $G_f\backslash\backslash S_n$ $\mathrm{Stab}(\mathcal{M}^\sigma)=G_f^\sigma(=\sigma^{-1}G_f\sigma)$. Moreover, we have the following:

Proposition 5. (1) *There exists exactly one primitive idempotent e of $\mathcal{A}_0$ such that $\mathcal{M}=\{g\in\mathcal{Q}[X]\mid eg\in\mathcal{M}_0\}$, where we consider e as an element in $\mathcal{Q}[X]$. For each σ in $G_f\backslash\backslash S_n$, $\mathcal{M}^\sigma=\{g\in\mathcal{Q}[X]\mid ge^\sigma\in\mathcal{M}_0\}$ and there is an isomorphism from $e^\sigma\mathcal{A}_0$ to $\mathcal{Q}[X]/\mathcal{M}^\sigma$ which maps $e^\sigma x_i$ to $x_i \bmod \mathcal{M}^\sigma$ and $\mathrm{Aut}_{\mathcal{Q}}(\mathcal{Q}[X]/\mathcal{M}^\sigma)=\mathrm{Aut}_{\mathcal{Q}}(e^\sigma\mathcal{A}_0)=\mathrm{Stab}(e^\sigma)=G_f^\sigma$. This relation gives a one-to-one correspondence between the set of all primitive idempotents of $\mathcal{A}_0$ and that of all prime divisors of $\mathcal{M}_0$. Thus,*

$$\mathcal{A}_0=\bigoplus_{\sigma\in G_f\backslash\backslash S_n} e^\sigma\mathcal{A}_0=\bigoplus_{\sigma\in G_f\backslash\backslash S_n}\mathcal{Q}[X]/\mathcal{M}^\sigma.$$

(2) *Let $\mathcal{S}$ be a subset of $G_f\backslash\backslash S_n$. Then*

$$\bigcap_{\sigma\in\mathcal{S}}\mathcal{M}^\sigma=\left\{g\in\mathcal{Q}[X]\,\middle|\, g\sum_{\sigma\in\mathcal{S}}e^\sigma\in\mathcal{M}_0\right\}.$$

This relation gives a one-to-one correspondence between the set of all idempotents of $\mathcal{A}_0$ and that of all radical ideals containing $\mathcal{M}_0$.

Proof. (1) Fix a primitive idempotent e' of $\mathcal{A}_0$ and consider the projection from $\mathcal{Q}[X]$ to $e'\mathcal{A}_0$ defined by $\mathcal{Q}[X] \to \mathcal{A}_0 \to e'\mathcal{A}_0$. Then its kernel is a maximal ideal and so it is a prime divisor, say $\mathcal{M}'$, of $\mathcal{M}_0$. Therefore, there is an element σ such that $\mathcal{M}' = \mathcal{M}^\sigma$. By the action of σ, we have $\mathcal{M} = \{g \mid ge'^{\sigma^{-1}} \in \mathcal{M}_0\}$. Setting e as $e'^{\sigma^{-1}}$, we have $\mathcal{M} = \{g \in \mathcal{Q}[X] \mid eg \in \mathcal{M}_0\}$. Moreover, $\mathrm{Stab}(e^\sigma \mathcal{A}_0) = \mathrm{Aut}_{\mathcal{Q}}(\mathcal{Q}[X]/\mathcal{M}^\sigma) = \mathrm{Stab}(\mathcal{M}^\sigma) = G_f^\sigma$.

(2) Let $e_{\mathcal{S}} = \sum_{\sigma\in\mathcal{S}} e^\sigma$ and $\mathcal{M}_{\mathcal{S}} = \bigcap_{\sigma\in\mathcal{S}} \mathcal{M}^\sigma$. For each polynomial $g(X)$ in $\mathcal{Q}[X]$, if $ge_{\mathcal{S}}$ belongs to $\mathcal{M}_0$, i.e., $ge_{\mathcal{S}} = 0$ in $\mathcal{A}_0$, then $0 = ge_{\mathcal{S}}e^\sigma = ge^\sigma$ in $\mathcal{A}_0$ for each σ. Thus g belongs to $\mathcal{M}_{\mathcal{S}}$. On the other hand, for each g belonging to $\mathcal{M}_{\mathcal{S}}$, $ge^\tau = 0$ in $\mathcal{A}_0$ for every τ in $\mathcal{S}$, and so $ge_{\mathcal{S}} = g\sum_{\sigma\in\mathcal{S}} e^\sigma = 0$ in $\mathcal{A}_0$. □

Definition 6. We say that an idempotent e of $\mathcal{A}_0$ *corresponds* with the ideal $\mathcal{M}$ if $\mathcal{M} = \{g \mid ge \in \mathcal{M}_0\}$.

Next, we define invariants of subgroups of S_n and resolvents. We use the following notation slightly modified from that used in [9, 25].

Definition 7. For a pair (H,L) of subgroups of S_n such that $H \subset L$, a polynomial P in $\mathcal{Q}[X]$ is an L-relative H-invariant if $\mathrm{Stab}_L(P) = H$. When $L = S_n$, we omit the word "S_n-relative". For an L-relative H-invariant P, we call the polynomial $\mathcal{L}_P^L$ defined below *the generic L-relative resolvent of P*:

$$\mathcal{L}_P^L(y) = \prod_{\tau\in H\backslash\backslash L} (y - P^\tau).$$

And we call its specialization at $(x_1,\dots,x_n) = (\alpha_1,\dots,\alpha_n)$ *the L-relative resolvent of P by f* and denote it by $\mathcal{L}_{P,f}^L$:

$$\mathcal{L}_{P,f}^L(y) = \phi(\mathcal{L}_{P,f}^L(y)) = \prod_{\tau\in H\backslash\backslash L} (y - \phi(P^\tau)).$$

For the case $L = S_n$, we call $\mathcal{L}_{P,f}^{S_n}$ the *absolute resolvent of P by f* and denote it simply by $\mathcal{L}_{P,f}$.

We note that if L contains G_f, $\mathcal{L}_{P,f}^L$ is a polynomial over $\mathcal{Q}$. The following gives the mathematical basis for methods for computing Galois groups based on resolvents (see its further extension [3]).

Theorem 8. *Let H and L be subgroups of S_n such that $G_f \subset L$ and $H \subset L$, and P an L-relative H-invariant. Suppose that $\phi(P^\sigma)$ is a simple root of $\mathcal{L}_{P,f}^L$ belonging to $\mathcal{Q}$ for some σ in $H\backslash\backslash L$. Then H^σ also contains G_f.*

Moreover, we have the following which is a refinement of [3, pp. 17, 18].

Corollary 9. *We use the same notation as in Theorem* 8 *and suppose that $H^\sigma = G_f$ and the characteristic of $\mathscr{Q}$ is* 0. *Then*

$$\mathscr{M} = \left(\bigcap_{\tau \in G_f \backslash\backslash L} \mathscr{M}^\tau \right) + Id(P^\sigma - \phi(P^\sigma)).$$

Definition 10. For a root A of the resolvent $\mathscr{L}_{P,f}$ belonging to $\mathscr{Q}$, we say that A *corresponds* with a prime divisor $\mathscr{M}^\sigma$ of $\mathscr{M}_0$ if $\phi(P^\sigma) = A$.

Remark 11. We recall useful properties of idempotents of $\mathscr{A}_0$.

(1) Primitive idempotents are orthogonal to each other.

(2) Every idempotent can be written uniquely as a sum of primitive idempotents. If an idempotent e' is written as $e' = e_1 + \cdots + e_t$ for primitive idempotents $e_1, \ldots, e_t$, we call each e_i a *component* of e'.

(3) A primitive idempotent e is a component of an idempotent e' if and only if $ee' \neq 0$. (If $ee' \neq 0$, then $ee' = e$.)

By Remark 1, we have the following:

Lemma 12. *Let e be the primitive idempotent corresponding to $\mathscr{M}$. Then, for each element g in $\mathscr{Q}[X]$, if $\phi(g)$ belongs to $\mathscr{Q}$, then $(\phi(g) - g)e = 0$ in $\mathscr{A}_0$. Especially, for a pair (H, L) of subgroups such that L contains H and G_f and for an L-relative H-invariant P, $(\mathscr{L}_P^L(y) - \mathscr{L}_{P,f}^L(y))e = 0$ in $\mathscr{A}_0[y]$.*

3. Splitting fields over p-adic number fields

Now, we consider the splitting rings over the field $\boldsymbol{Q}$ of rational numbers and the p-adic number field and show that the values of invariants can be lifted from their modular images over finite fields. From now on, we suppose that f is a square-free, monic polynomial over the ring $\boldsymbol{Z}$ of integers, and fix $\Omega_f = \{\alpha_1, \ldots, \alpha_n\}$ and the splitting ideal $\mathscr{M}$ associated with the assignment x_i to α_i. For a prime integer p, we denote by $\boldsymbol{Z}_p^0$, $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ the localization of $\boldsymbol{Z}$ at p, the completion of $\boldsymbol{Z}_p^0$ and the p-adic number field, respectively. We denote by π_p the projection from $\boldsymbol{Z}_p[X]$ to $GF(p)[X]$ which is the natural extension of the projection from $\boldsymbol{Z}$ to $GF(p)$.

3.1. Relations among universal splitting rings

We fix a prime number p such that $\pi_p(f)$ is square-free, i.e., p does not divide the discriminant $d(f)$ of f, and let $\pi = \pi_p$. Let $\bar{\mathscr{M}}_0$ denote the ideal $\pi(\mathscr{M}_0 \cap \boldsymbol{Z}[X])$ in $GF(p)[X]$ and $\mathscr{G}_0$ denote the standard generating set of $\mathscr{M}_0$. Then $\pi(\mathscr{G}_0)$ exists and it is the Gröbner basis of the ideal generated by itself. Since M-reductions of polynomials in $\boldsymbol{Z}_p[X]$ with respect to $\mathscr{G}_0$ can be done over $\boldsymbol{Z}_p$, we can easily show the following related to the notion of *compatibility* of primes with Gröbner bases in [20].

Lemma 13. *The universal splitting ideal of* $\pi(f)$ *over* $GF(p)$ *coincides with* $\bar{\mathscr{M}}_0$ *and* $\pi(\mathscr{G}_0)$ *is the standard generating set of* $\bar{\mathscr{M}}_0$. *Moreover,* $\mathscr{G}_0$ *is the standard generating set of the universal splitting ideal* $\boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} \mathscr{M}_0$ *over* $\boldsymbol{Q}_p$ *and that of* $\boldsymbol{Z}_p[X] \otimes_{\boldsymbol{Z}_p^0} (\mathscr{M}_0 \cap \boldsymbol{Z}_p^0[X])$ *over* $\boldsymbol{Z}_p$.

We denote universal splitting ideals $\boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} \mathscr{M}_0$ over $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p[X] \otimes_{\boldsymbol{Z}_p^0} (\mathscr{M}_0 \cap \boldsymbol{Z}_p^0[X])$ over $\boldsymbol{Z}_p$ by $\mathscr{M}_0^{(\infty)}$ and $\mathscr{M}_0^{(\infty)+}$, respectively. And we denote the universal splitting rings $GF(p)[X]/\bar{\mathscr{M}}_0$, $\boldsymbol{Z}_p[X]/\mathscr{M}^{(\infty)+}$ and $\boldsymbol{Q}_p[X]/\mathscr{M}^{(\infty)}(=\boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} \mathscr{A}_0)$ by $\bar{\mathscr{A}}_0$, $\mathscr{A}_0^{(\infty)+}$ and $\mathscr{A}_0^{(\infty)}$, respectively. As the representative of each residue class, we use the normal form of elements in the residue class with respect to the standard generating set.

Lemma 14. *Each element of* $\mathscr{A}_0$, $\mathscr{A}_0^{(\infty)}$, $\mathscr{A}_0^{(\infty)+}$ *and* $\bar{\mathscr{A}}_0$ *is expressed as a linear sum of terms* $x_1^{e_1} \cdots x_n^{e_n}$ *such that* $0 \le e_i \le n-i$ *for* $i = 1, \ldots, n$. *For each* g *in* $\boldsymbol{Z}_p[X]$, *the representative of the residue class containing* g *belongs* $\boldsymbol{Z}_p[X]$.

Using representatives, we can treat elements in universal splitting rings as elements in the original polynomial rings. By Lemma 14 we can extend the projection π to $\mathscr{A}_0^{(\infty)+}$. Then $\bar{\mathscr{M}}_0 \equiv \mathscr{M}_0^{(\infty)+}/p\mathscr{M}_0^{(\infty)+}$ and $\bar{\mathscr{A}}_0 \equiv \mathscr{A}_0^{(\infty)+}/p\mathscr{A}_0^{(\infty)+}$.

Lemma 15. *Every idempotent* $e^{(\infty)}$ *of* $\mathscr{A}_0^{(\infty)}$ *belongs to* $\mathscr{A}_0^{(\infty)+}$ *and* $\pi(e^{(\infty)}) \neq 0$.

Proof. Assume, to the contrary, that some idempotent $e^{(\infty)}$ of $\mathscr{A}_0^{(\infty)}$ does not belong to $\mathscr{A}_0^{(\infty)+}$. Let k be the smallest positive integer such that $p^k e^{(\infty)}$ belongs to $\mathscr{A}_0^{(\infty)+}$ and set $u = p^k e^{(\infty)}$. As $e^{(\infty)}(e^{(\infty)} - 1) = 0$, we have $u^2 = p^k u$ in $\mathscr{A}_0^{(\infty)+}$ and so u^2 belongs to $p^k \mathscr{A}_0^{(\infty)+}$. Now consider $\pi(u)$ in $\bar{\mathscr{A}}_0$. By the definition of u, $\pi(u) \neq 0$. However, $(\pi(u))^2 = \pi(u^2) = 0$ in $\bar{\mathscr{A}}_0$. Since $\pi(f)$ is square-free, $\bar{\mathscr{A}}_0$ is the direct sum of fields (see Proposition 5). From this, we can show that $(\pi(u))^2 = 0$ implies $\pi(u) = 0$. This is a contradiction.

Next, we show $\pi(e^{\infty}) \neq 0$. Assume the contrary $\pi(e^{(\infty)}) = 0$. Then $e^{(\infty)}$ can be written as pu for some u in $\mathscr{A}_0^{(\infty)+}$. As $e^{(\infty)}(e^{(\infty)} - 1) = 0$, $e^{(\infty)} = p^2 u^2$. Repeating this replacement, $e^{(\infty)} = p^{2^k} u^{2^k}$ for any positive integer k. This implies $e^{(\infty)} = 0$ and a contradiction. □

Theorem 16. *The projection* π *gives a one-to-one correspondence between the set of all primitive idempotents of* $\mathscr{A}_0^{(\infty)}$ *and that of* $\bar{\mathscr{A}}_0$. *Moreover, for each pair* $(\bar{e}, e^{(\infty)})$ *of corresponding primitive idempotents,* $\mathrm{Stab}(\bar{e}) = \mathrm{Stab}(e^{(\infty)})$.

We will give a proof of Theorem 16 in Section 3.2.

Proposition 17. (1) *For each primitive idempotent e of $\mathscr{A}_0$, e is also an idempotent of $\mathscr{A}_0^{(\infty)}$ and $\pi(e)$ is also an idempotent of $\bar{\mathscr{A}_0}$ (this corresponds with* [21, p. 127]).

(2) *Let $\bar{e}$ be a component of $\pi(e)$ and let $e^{(\infty)}$ be the primitive idempotent of $\mathscr{A}_0^{(\infty)}$ corresponding to $\bar{e}$. Then* $\mathrm{Stab}(e)$ *contains* $\mathrm{Stab}(\bar{e})$ $(=\mathrm{Stab}(e^{(\infty)}))$ *and* $\mathrm{Stab}(\pi(e)) = \mathrm{Stab}(e)$. *Moreover, by letting $\mathscr{S}=\mathrm{Stab}(\bar{e})\backslash\backslash\mathrm{Stab}(e)$,*

$$\pi(e)=\sum_{\sigma\in\mathscr{S}}\bar{e}^{\sigma} \quad \textit{and} \quad e=\sum_{\sigma\in\mathscr{S}}e^{(\infty)^{\sigma}}.$$

Proof. (1) As e^2-e belongs to $\mathscr{M}_0\subset\mathscr{M}_0^{(\infty)}$, e is also an idempotent of $\mathscr{A}_0^{(\infty)}$. Then e is written as a sum of primitive idempotents of $\mathscr{A}_0^{(\infty)}$. By Lemma 15, $\pi(e)$ exists and $\pi(e)^2=\pi(e^2)=\pi(e)$.

(2) Let $\mathscr{E}=\{e_1(=e),\dots,e_r\}$ be the set of all primitive idempotents of $\mathscr{A}_0$ and let $\bar{\mathscr{E}}$ be that of $\bar{\mathscr{A}_0}$. Then $|\mathscr{E}|=[S_n:G_f]$ and $|\bar{\mathscr{E}}|=[S_n:\mathit{Stab}(\bar{e})]$. Let $\bar{\mathscr{E}_i}$ be the set of all components of $\pi(e_i)$ for each i, $i=1,\dots,r$. Since e_i's are orthogonal to each other and $e_1+\cdots+e_r=1$, $\pi(e_i)$'s are orthogonal to each other and $\pi(e_1)+\cdots+\pi(e_r)=1$. Therefore, $\bar{\mathscr{E}_1},\dots,\bar{\mathscr{E}_r}$ are disjoint and $\bar{\mathscr{E}}=\bigcup_{i=1}^{r}\bar{\mathscr{E}_i}$. And $\bar{\mathscr{E}_i}$'s are conjugate to each other in S_n. Thus, $|\bar{\mathscr{E}_1}|=|\bar{\mathscr{E}}|/r=[S_n:\mathrm{Stab}(\bar{e})]/[S_n:G_f]=|G_f|/|\mathrm{Stab}(\bar{e})|=|\mathrm{Stab}(e)|/|\mathrm{Stab}(\bar{e})|$. On the other hand, for each σ in $\mathrm{Stab}(e), \bar{e}^{\sigma}\pi(e)=\bar{e}^{\sigma}\pi(e^{\sigma})=(\bar{e}\pi(e))^{\sigma}=\bar{e}^{\sigma}$, that is, $\bar{e}^{\sigma}$ is also a component of $\pi(e)$. Thus, $|\bar{\mathscr{E}_1}|\geq[\mathrm{Stab}(e):\mathrm{Stab}(\bar{e})\cap\mathrm{Stab}(e)]\geq|\mathrm{Stab}(e)|/|\mathrm{Stab}(\bar{e})|$. This shows that $\mathrm{Stab}(\bar{e})$ is contained in $\mathrm{Stab}(e)$ and $\bar{\mathscr{E}_1}$ consists of all $\mathrm{Stab}(e)$-conjugates to $\bar{e}$, i.e., $\pi(e)=\sum_{\sigma\in\mathscr{S}}\bar{e}^{\sigma}$. Moreover, $\mathrm{Stab}(e)=\mathrm{Stab}(\pi(e))$.

Finally, we show $e=\sum_{\sigma\in\mathscr{S}}(e^{(\infty)})^{\sigma}$. By Remark 11, it suffices to show that for each primitive idempotent $e^{(\infty)'}$ of $\mathscr{A}_0^{(\infty)}$, $e^{(\infty)'}e\neq0$ if and only if $e^{(\infty)'}$ is $\mathrm{Stab}(e)$-conjugate to $e^{(\infty)}$. Since $\pi(e)\bar{e}^{\sigma}=\bar{e}^{\sigma}$ for $\sigma\in\mathscr{S}$, we have $e(e^{(\infty)})^{\sigma}\neq0$. Conversely, if $e^{(\infty)'}e\neq0$ then $e^{(\infty)'}e=e^{(\infty)'}$ and so $\pi(e^{(\infty)'})\bar{e}=\pi(e^{(\infty)'})\neq0$. This implies that $\pi(e^{(\infty)'})=\bar{e}^{\sigma}$ for some σ in $\mathrm{Stab}(e)$ and $e^{(\infty)'}=(e^{(\infty)})^{\sigma}$. □

Lemma 18. *Let e be the primitive idempotent corresponding to $\mathscr{M}$. Consider a polynomial g in $\boldsymbol{Z}[X]$ such that $\phi(g)$ belongs to $\boldsymbol{Q}$. Then $(g-\phi(g))e^{(\infty)}=0$ for every component $e^{(\infty)}$ of e and $(\pi(g)-\pi(\phi(g)))\bar{e}=0$ for every component $\bar{e}$ of $\pi(e)$. Especially, for the generic L-relative resolvent of P, where L and H are subgroup of S_n such that L contains H and G_f and P is an L-relative H-invariant, $(\mathscr{L}_{P,f}^{L}-\mathscr{L}_{P}^{L})e^{(\infty)}=0$ and $(\pi(\mathscr{L}_{P,f}^{L})-\pi(\mathscr{L}_{P}^{L}))\bar{e}=0$.*

Proof. Since $\phi(g)$ is an algebraic integer, $\phi(g)$ belongs to $\boldsymbol{Z}$. By Lemma 12, $(g-\phi(g))e=0$ in $\mathscr{A}_0$. Then $(g-\phi(g))ee^{(\infty)}=(g-\phi(g))e^{(\infty)}=0$ in $\mathscr{A}_0^{(\infty)}$ for any component $e^{(\infty)}$ of e. Moreover, by Theorem 16 we have $(\pi(g)-\pi(\phi(g))\bar{e}=0$ for every component $\bar{e}$ of $\pi(e)$. □

By combining Theorems 8 and 17, we have the following.

Theorem 19. *Let H and L be subgroups of S_n such that L contains G_f and H, P an L-relative H-invariant in $\boldsymbol{Z}[X]$, e the primitive idempotent corresponding to $\mathscr{M}$ and*

$e^{(\infty)}$ a component of e in $\mathscr{A}_0^{(\infty)}$. Suppose that $(P^\sigma - A)e^{(\infty)} = 0$ for an integer A and some σ in $H\backslash\backslash L$, and $P^\sigma e^{(\infty)} \neq P^{\sigma'} e^{(\infty)}$ for any $\sigma' \neq \sigma$ in $H\backslash\backslash L$. Then H^σ contains G_f and $(P^\sigma - A)e = 0$, i.e., $\phi(P^\sigma) = A$.

Proof. Consider the generic L-relative resolvent $\mathscr{L}_P^L(y)$ of P. Then L fixes $\mathscr{L}_P^L(y)$. By the assumption $(P^\sigma - A)e^{(\infty)} = 0$, we have $\mathscr{L}_P^L(A)e^{(\infty)} = 0$ and so $\mathscr{L}_P^L(A)e^{(\infty)\tau} = (\mathscr{L}_P^L(A)e^{(\infty)})^\tau = 0$ for any τ in L. By the fact that $e = \sum_{\tau \in \mathrm{Stab}(e^{(\infty)})\backslash\backslash \mathrm{Stab}(e)} e^{(\infty)\tau}$ and by using Lemma 12 we obtain

$$\mathscr{L}_{P,f}^L(A)e = \mathscr{L}_P^L(A)e = \sum_{\tau \in \mathrm{Stab}(e^{(\infty)})\backslash\backslash \mathrm{Stab}(e)} \mathscr{L}_P^L(A)e^{(\infty)\tau} = 0.$$

Thus, A is an integral root of $\mathscr{L}_{P,f}^L$, i.e., for some τ in $H\backslash\backslash L$, $\phi(P^\tau) - A = 0$ and so $(P^\tau - A)e = 0$. As $e^{(\infty)}$ is a component of e, $(P^\tau - A)e^{(\infty)} = 0$. On the other hand, since $P^\sigma e^{(\infty)} \neq P^{\sigma'} e^{(\infty)}$ for any σ' with $H\sigma \neq H\sigma'$, this implies that $\tau = \sigma$ and so A is a simple root of $\mathscr{L}_{P,f}^L$. Thus H^σ contains G_f. □

3.2. Lifting procedures

First we prove Theorem 16 by showing that each idempotent of $\bar{\mathscr{A}_0}$ can be lifted to its corresponding idempotent of $\mathscr{A}_0^{(\infty)}$. Then we consider how we can construct values of invariants over K_f by their modular images.

Theorem 20. *The projection π gives a one-to-one correspondence between the set of all idempotents of $\mathscr{A}_0^{(\infty)}$ and that of $\bar{\mathscr{A}_0}$. Moreover, each idempotent of $\bar{\mathscr{A}_0}$ can be lifted to its corresponding idempotent of $\mathscr{A}_0^{(\infty)}$ by Hensel construction.*

Proof. By Lemma 15, it suffices to show that for each idempotent $\bar{e}$ of $\bar{\mathscr{A}_0}$ there is exactly one idempotent $e^{(\infty)}$ of $\mathscr{A}_0^{(\infty)}$ such that $\pi(\bar{e}^{(\infty)}) = \bar{e}$ and it can be constructed from $\bar{e}$ by Hensel construction. So, we consider $\mathscr{A}^{(\infty)+}$.

First we show the existence. To do it, we show that there is an element $e^{(i)}$ in $\mathscr{A}_0^{(\infty)+}$ such that $e^{(i)} \equiv \bar{e} \pmod p$ and $(e^{(i)})^2 \equiv e^{(i)} \pmod{p^{i+1}}$ for any non-negative integer i by induction argument which describes a Hensel construction procedure. Let $e^{(0)}$ be an inverse image of $\bar{e}$ in $\mathscr{A}_0^{(\infty)+}$. Then $(e^{(0)})^2 \equiv e^{(0)} \pmod p$, which shows the claim for $i = 0$. So assume that the claim is true for $i \geq 0$. Then there is an element $e^{(i)}$ such that $e^{(i)} \equiv \bar{e} \pmod p$ and $(e^{(i)})^2 \equiv e^{(i)} \pmod{p^{i+1}}$. Set $\Delta_i = ((e^{(i)})^2 - e^{(i)}))/p^{i+1}$, $\Gamma_{i+1} = (-2e^{(0)} + 1)\Delta_i$ and $e^{(i+1)} = e^{(i)} + p^{i+1}\Gamma_{i+1}$. Since $(2e^{(0)} - 1)(2e^{(0)} - 1) = 4(e^{(0)})^2 - 4e^{(0)} + 1 \equiv 1 \pmod p$, we obtain

$$((e^{(i+1)})^2 - e^{(i+1)})/p^{i+1} \equiv \Delta_i(1 - (2e^{(0)} - 1)(2e^{(0)} - 1)) \equiv 0 \pmod p.$$

Thus $e^{(i+1)}$ satisfies the condition of the claim.

Next, we show the uniqueness of the lifted idempotent. Since $(2\bar{e} - 1)$ is invertible in $\bar{\mathscr{A}_0}$, the difference $p^{i+1}\Gamma_{i+1}$ between $e^{(i)}$ and $e^{(i+1)}$ is determined uniquely modulo p by Δ_i at each step i. This assures the uniqueness of $e^{(\infty)}$. □

Proof of Theorem 16. First we show that for each primitive idempotent $\bar{e}$, its lifted idempotent $e^{(\infty)}$ is primitive. Assume that $e^{(\infty)}$ is written as $e_1^{(\infty)} + \cdots + e_s^{(\infty)}$ for primitive idempotents $e_1^{(\infty)},\dots,e_s^{(\infty)}$. Then $\bar{e} = \pi(e^{(\infty)}) = \pi(e_1^{(\infty)}) + \cdots + \pi(e_s^{(\infty)})$. As $\bar{e}$ is primitive and $\pi(e_i^{(\infty)}) \neq 0$ for every i, we obtain $s = 1$, that is, $e^{(\infty)}$ is primitive. By the similar argument as in the above, we can show that for each primitive idempotent $e^{(\infty)}$, its image $\bar{e} = \pi(e^{(\infty)})$ is also primitive. Thus, π gives a one-to-one correspondence between the set of all primitive idempotents of $\mathscr{A}_0^{(\infty)}$ and that of $\bar{\mathscr{A}}_0$.

Next, we show $\mathrm{Stab}(\bar{e}) = \mathrm{Stab}(e^{(\infty)})$. Since the number of primitive idempotents of $\mathscr{A}_0^{(\infty)}$ coincides with $[S_n : \mathrm{Stab}(e^{(\infty)})]$ and that of $\bar{\mathscr{A}}_0$ coincides with $[S_n : \mathrm{Stab}(\bar{e})]$, we have $[S_n : \mathrm{Stab}(e^{(\infty)})] = [S_n : \mathrm{Stab}(\bar{e})]$ by the one-to-one correspondence. Meanwhile, as $\bar{e} = \pi(e^{(\infty)})$, $\mathrm{Stab}(e^{(\infty)})$ also stabilizes $\bar{e}$, i.e., $\mathrm{Stab}(e^{(\infty)}) \subset \mathrm{Stab}(\bar{e})$. Comparing the orders, we get $\mathrm{Stab}(\bar{e}) = \mathrm{Stab}(e^{(\infty)})$. □

Now, we fix a primitive idempotent $\bar{e}$ of $\bar{\mathscr{A}}_0$. Let $\bar{\mathscr{M}}$ be its corresponding maximal ideal of $GF(p)[X]$ and $\bar{\mathscr{G}} = \{\bar{g}_1,\dots,\bar{g}_n\}$ the reduced Gröbner basis of $\bar{\mathscr{M}}$ with respect to the lexicographic order $<$ such that $x_1 < \cdots < x_n$. We will lift $\bar{\mathscr{G}}$ to its counterpart in $\mathbf{Z}_p[X]$. Let $e^{(\infty)}$ be the lifted idempotent of $\bar{e}$ and $\mathscr{M}^{(\infty)}$ its corresponding splitting ideal.

Theorem 21. *The Gröbner basis $\bar{\mathscr{G}}$ is lifted uniquely to the Gröbner basis of $\mathscr{M}^{(\infty)}$ with respect to $<$ by Hensel construction.*

Proof. By induction on i, we show that for each $\bar{g}_i$, there is exactly one polynomial $g_i^{(\infty)}$ in $\mathbf{Z}_p[X]$ such that $\pi(g_i^{(\infty)}) = \bar{g}_i$ and $g_i^{(\infty)}(x_1,\dots,x_{i-1},x)$ is a monic irreducible factor of $f(x)$ over $\mathbf{Q}_p[x_1,\dots,x_{i-1}]/Id(\mathscr{G}_{i-1}^{(\infty)})$, where $\mathscr{G}_{i-1}^{(\infty)} = \{g_1^{(\infty)},\dots,g_{i-1}^{(\infty)}\}$, and $g_i^{(\infty)}$ is lifted from $\bar{g}_i$ by Hensel construction.

For the case $i = 1$, since $\pi(f)$ is square-free, the claim can be shown by *the ordinary* Hensel construction. So let $i > 1$ and assume that the claim holds for $i - 1$. By modifying the Hensel construction proposed by [26] to the successive extension case, we obtain a procedure which lifts $\bar{g}_i(x_1,\dots,x_i)$ to $g_i^{(\infty)}(x_1,\dots,x_i)$ in $\mathbf{Z}_p[x_1,\dots,x_i]$. Here we give an outline of the procedure.

We set $g_i^{(0)} = \bar{g}_i$ and $h_i^{(0)} = \bar{h}_i$ as elements of $\mathbf{Z}_p[X]$, where $\bar{h}_i$ is the cofactor of $\bar{g}_i$. Assume that for some integer $k \geq 0$, we constructed $g_i^{(k)}$ and $h_i^{(k)}$ such that $\deg_{x_i}(g_i^{(k)}) = \deg_{x_i}(\bar{g}_i)$, $\deg_{x_i}(h_i^{(k)}) = \deg_{x_i}(\bar{h}_i)$ and

$$f(x_i) \equiv g_i^{(k)}(x_1,\dots,x_i)h_i^{(k)}(x_1,\dots,x_i)\,(\mathrm{mod}\, p^{k+1}, Id(\mathscr{G}_{i-1}^{(\infty)}) \cap \mathbf{Z}_p[X]).$$

As $\gcd(\bar{g}_i, \bar{h}_i) = 1$ over the field $GF(p)[x_1,\dots,x_{i-1}]/Id(\bar{g}_1,\dots,\bar{g}_{i-1})$, there are $g_{i,k+1}$, $h_{i,k+1}$ such that $\deg_{x_i} g_{i,k+1} < \deg_{x_i} \bar{g}_i$, $\deg_{x_i} h_{i,k+1} < \deg_{x_i} \bar{h}_i$ and

$$\pi(u) - \bar{g}_i\pi(h_{i,k+1}) - \bar{h}_i\pi(g_{i,k+1}) \equiv 0, \quad (\mathrm{mod}\, Id(\bar{g}_1,\dots,\bar{g}_{i-1})),$$

where $u = \mathrm{NF}_{\mathscr{G}_{i-1}^{(\infty)}}(f(x_i) - g_i^{(k)}h_i^{(k)})/p^{k+1}$. Letting $g_i^{(k+1)} = g_i^{(k)} + p^{k+1}g_{i,k+1}$ and $h_i^{(k+1)} = h_i^{(k)} + p^{k+1}h_{i,k+1}$, we can show easily that

$$f(x_i) \equiv g_i^{(k+1)}(x_1,\dots,x_i)h_i^{(k+1)}(x_1,\dots,x_i)\,(\mathrm{mod}\, p^{k+2}, Id(\mathscr{G}_{i-1}^{(\infty)}) \cap \boldsymbol{Z}_p[X]).$$

By continuing this procedure, we finally have $\bar{g}_i^{(\infty)}$. The irreducibility of $g_i^{(\infty)}$ follows from that of $\bar{g}_i$ and its uniqueness can be shown by the uniqueness of $\pi(g_{i,k+1})$ and $\pi(h_{i,k+1})$ in the extended GCD computation, see [26].

Next, consider the prime decomposition of $\mathscr{M}_0^{(\infty)}$. By the correspondence of prime divisors and primitive idempotents, we can show that $Id(\mathscr{G}^{(\infty)})e^{(\infty)} = 0$ in $\mathscr{A}_0^{(\infty)}$ and so $\mathscr{G}^{(\infty)}$ is the Gröbner basis of $\mathscr{M}^{(\infty)}$. □

In the Hensel construction procedure, for each k and i, we can replace the normal form with respect to $\mathscr{G}_{i-1}^{(\infty)}$ by the normal form with respect to $\mathscr{G}_{i-1}^{(k+1)}$, where $\mathscr{G}_i^{(k)} = \{g_1^{(k)},\dots,g_i^{(k)}\}$. Thus, in actual computation, we use a Hensel construction which lifts $\mathscr{G}^{(k)}$ to $\mathscr{G}^{(k+1)}$ for each k, where $\mathscr{G}^{(k)} = \mathscr{G}_n^{(k)}$.

Definition 22. We call the above $\mathscr{G}^{(k)}$ a *kth approximation to* $\mathscr{G}^{(\infty)}$.

For each polynomial P in $\boldsymbol{Q}[X]$, $\mathrm{NF}_{\mathscr{G}^{(\infty)}}(P)$ is considered as the evaluation of P over the extension field $\boldsymbol{Q}_p[X]/\mathscr{M}^{(\infty)}$. This implies that we can lift the value $\phi(P)$ from its image $\pi(\phi(P))$ by Hensel construction.

Corollary 23. *Let H and L be subgroups of S_n such that L contains H and G_f, P an L-relative H-invariant in $\boldsymbol{Z}[X]$ and e the primitive idempotent corresponding to $\mathscr{M}$. Then,*

(1) *If $\pi(\mathscr{L}_{P,f}^L)$ has a root in $GF(p)$ with multiplicity v, it can be lifted to v roots of $\mathscr{L}_{P,f}^L$ in a splitting field of f over $\boldsymbol{Q}_p$.*

(2) *Suppose that $(\pi(P^\sigma) - \bar{A})\bar{e} = 0$, where $\bar{A} \in GF(p)$, for some σ in L and a component $\bar{e}$ of $\pi(e)$, and $\bar{A}$ is lifted to a simple integral root A of $\mathscr{L}_{P,f}^L$ over $e^{(\infty)}\mathscr{A}_0^{(\infty)}$, where $e^{(\infty)}$ is the lifted idempotent of $\bar{e}$. Then H^σ contains G_f. If none of the roots of $\pi(\mathscr{L}_{P,f}^L)$ in $GF(p)$ is lifted to an integral root of $\mathscr{L}_{P,f}^L$, then G_f is not contained in any L-conjugates of H.*

4. Finding Galois groups

Here we present a new method based on Stauduhar's approach. Let $f(x)$ be a square-free, monic integral polynomial of degree n, $\mathscr{M}_0$ its universal splitting ideal, and p a prime which does not divide the discriminant of f.

By using methods for algebraic factoring over finite fields (see a survey [14]), we *compute* a prime divisor $\bar{\mathscr{M}}$ of the universal splitting ideal $\bar{\mathscr{M}}_0$ of $\pi_p(f)$ over $GF(p)$, that is, we compute the Gröbner basis $\bar{\mathscr{G}}$ of $\bar{\mathscr{M}}$. Let $\bar{e}$ be the primitive idempotent corresponding to $\bar{\mathscr{M}}$. Then there is a pair $(\mathscr{M}, e)$ of a prime divisor $\mathscr{M}$ of

$\mathscr{M}_0$ and its corresponding primitive idempotent e such that $\mathscr{M}$ is a prime divisor of the ideal $\pi_p(\mathscr{M}\cap \boldsymbol{Z}_p[X])$ and $\bar{e}$ is a component of the idempotent $\pi_p(e)$. By Theorems 20 and 21, there is the lifted Gröbner basis $\mathscr{G}^{(\infty)}$ of the maximal ideal $\mathscr{M}^{(\infty)}$ corresponding to the lifted primitive idempotent $e^{(\infty)}$. In the new method, we never compute idempotents, but we lift $\bar{\mathscr{G}}$ to an approximation $\mathscr{G}^{(k)}$ to $\mathscr{G}^{(\infty)}$ for a certain degree k.

We fix the Galois groups G_f and $G_{\pi_p(f)}$ as $\mathrm{Stab}(e)$ and $\mathrm{Stab}(\bar{e})$, respectively. We also fix an assignment $\alpha_1 \to x_1,\dots,\alpha_n \to x_n$ such that the assignment can be extended to an isomorphism from $\boldsymbol{Q}(\alpha_1,\dots,\alpha_n)$ to $\boldsymbol{Q}[X]/\mathscr{M}$. By this assignment, $\phi(P)$ becomes an integer A if and only if $(P-A)e=0$ in $\mathscr{A}_0$. Moreover, $(\pi_p(P)-\pi_p(A))\bar{e}=0$ in $\bar{\mathscr{A}}_0$ and $\pi_p(A)=\mathrm{NF}_{\bar{\mathscr{G}}}(\pi_p(P))$ in $GF(p)[X]$. Now we assume that we can do the following group computation:

(i) For any subgroup L of S_n we can compute all conjugate classes of maximal subgroups of L. (If f is irreducible, we need only transitive subgroups.)

(ii) For any pair (L,H) of subgroups of S_n such that L contains H, we can compute the set $H\backslash\backslash L$ of all representatives of the right coset $H\backslash L$.

Applying the following procedure repeatedly from the *initial* setting $L=S_n$, we obtain the Galois group G_f.

```
Procedure ($L$, $\mathscr{G}^{(k)}$)
  Inputs: a subgroup $L$ of $S_n$ and a $k$th approximation $\mathscr{G}^{(k)}$.
  Assumption: $L$ contains $G_f$.
  Output: a maximal subgroup $H$ of $L$ containing $G_f$ if exists, and $L$, otherwise.
   (1) Compute the list $\mathscr{C}$ of all conjugate classes of maximal subgroups of $L$.
   (2) For each maximal subgroup $H$ in $\mathscr{C}$, do:
       (2.1) Compute $H\backslash\backslash L$.
       (2.2) Compute an $L$-relative $H$-invariant $P$ in $\boldsymbol{Z}[X]$ and a bound $M$ such that
             $2[L:H]<M$ and $|\phi(P^\sigma)|<M$ for every $\sigma$ in $H\backslash\backslash L$.
       (2.3) Compute $\mathrm{NF}_{\pi_p(\mathscr{G}^{(k)})}(\pi_p(P^\sigma))$ in $GF(p)[X]$ for every $\sigma$ in $H\backslash\backslash L$ and let
             $\mathscr{S}_0=\{\sigma\in H\backslash\backslash L \mid \mathrm{NF}_{\pi_p(\mathscr{G}^{(k)})}(\pi_p(P^\sigma))\in GF(p)\}$.
       (2.4) If $\mathscr{S}_0=\emptyset$, then go to (2).
       (2.5) If $p^{k+1}<(2M)^{[L:H]}$, then lift $\mathscr{G}^{(k)}$ to $\mathscr{G}^{(k')}$ for $k'$ such that $p^{k'+1}>$
             $(2M)^{[L:H]}$ and replace $\mathscr{G}^{(k)}$ by $\mathscr{G}^{(k')}$.
       (2.6) Compute $A_\sigma=\mathrm{NF}_{\mathscr{G}^{(k)}}(P^\sigma)$ for all $\sigma$ in $H\backslash\backslash L$ and let $\mathscr{S}=\{\sigma\in H\backslash\backslash L \mid A_\sigma\in\boldsymbol{Z}$
             and $|A_\sigma|<M\}$. ($A_\sigma$ is given as an integer between $-(p^{k+1}-1)/2$ and
             $p^{k+1}/2$.)
       (2.7) If $\mathscr{S}=\emptyset$ then go to (2).
       (2.8) If there is $\sigma$ in $\mathscr{S}$ such that $A_\sigma\neq A_{\sigma'}$ for any $\sigma'$ in $\mathscr{S}\backslash\{\sigma\}$, then return
             $H^\sigma$ and otherwise, go to (2.2). (We have to use another $P$.)
   (3) Return $L$ as $G_f$.
```

Now, we show the correctness of this procedure, where the decisions on whether H^σ contains G_f are given at Steps (2.4), (2.7) and (2.8).

Correctness of the decision at Steps (2.4) and (2.7). Suppose that H^σ contains G_f. Then $A=\phi(P^\sigma)$ is an integer and $\pi_p(A)$ is an element of $GF(p)$. By Lemma 18, $(\pi_p(P^\sigma)-\pi_p(A))\bar{e}=0$ and so $\mathrm{NF}_{\bar{\mathscr{G}}}(\pi_p(P^\sigma))=\pi_p(A)$. This shows the correctness of the decision at Step (2.4). Also by Lemma 18, $(P^\sigma - A)e^{(\infty)}=0$ and so $\mathrm{NF}_{\mathscr{G}^{(\infty)}}(P^\sigma)=A$. As $\mathscr{G}^{(k)} \equiv \mathscr{G}^{(\infty)} \pmod{p^{k+1}}$, $\mathrm{NF}_{\mathscr{G}^{(k)}}(P^\sigma)\equiv A \pmod{p^{k+1}}$. Moreover, by the definition of M, $|A|<M$, which shows the correctness of the decision at Step (2.7).

Correctness of the decision at Step (2.8). Consider the resolvent $\mathscr{L}^L_{P,f}$ over $\boldsymbol{Q}$. By the construction of A_σ, $(P^\sigma - A_\sigma)e^{(\infty)}\equiv 0 \pmod{p^{k+1}}$. Since $\mathscr{L}^L_{P,f}(y)e^{(\infty)}=\prod_{\tau\in H\backslash\backslash L}(y-\mathrm{NF}_{\mathscr{G}^{(\infty)}}(P^\tau))e^{(\infty)}$ by Lemma 18, we have

$$\mathscr{L}^L_{P,f}(A_\sigma)e^{(\infty)}\equiv 0 \pmod{p^{k+1}}.$$

We note that each τ in L fixes $\mathscr{L}^L_P(y)$ and so it also fixes $\mathscr{L}^L_P(A_\sigma)$. As L contains G_f, for each τ in G_f we have $\mathscr{L}^L_P(A_\sigma)e^{(\infty)\tau}\equiv 0 \pmod{p^{k+1}}$. By Lemma 12,

$$\mathscr{L}^L_{P,f}(A_\sigma)e=\mathscr{L}^L_P(A_\sigma)e=\sum_{\tau\in \mathrm{Stab}(e^{(\infty)})\backslash\backslash G_f}\mathscr{L}^L_P(A_\sigma)e^{(\infty)\tau}\equiv 0 \pmod{p^{k+1}}.$$

This implies that $\mathscr{L}^L_{P,f}(y)=(y-A_\sigma)h(y)+p^{k+1}u(y)$ for some polynomials h,u in $\boldsymbol{Z}[y]$. Thus, $\mathscr{L}^L_{P,f}(A_\sigma)=0$ or $|\mathscr{L}^L_{P,f}(A_\sigma)|\geq p^{k+1}$.

On the other hand, as $\mathscr{L}^L_{P,f}(A_\sigma)=\prod_{\tau\in H\backslash\backslash L}(A_\sigma-\phi(P^\tau))$, we have $|\mathscr{L}^L_{P,f}(A_\sigma)|<(2M)^{[L:H]}$. By the choice of k, $\mathscr{L}^L_{P,f}(A_\sigma)=0$ and so A_σ is an integral root of $\mathscr{L}^L_{P,f}$. Then there is some σ in $H\backslash\backslash L$ such that $(P^{\sigma'}-A_\sigma)e=0$ and so $(P^{\sigma'}-A_\sigma)e^{(\infty)}=0$. From this, $\mathrm{NF}_{\mathscr{G}^{(k)}}(P^{\sigma'})=A_\sigma$. The condition that $A_\sigma\neq A_{\sigma'}$ for any σ' in $\mathscr{S}\backslash\{\sigma\}$, implies that $\sigma'=\sigma$ and A_σ is a simple integral root of $\mathscr{L}^L_{P,f}$. Thus, H^σ contains G_f by Theorem 8.

How to compute the bound *M*. Here, we give a simple bound M for a given L-relative H-invariant P in $\boldsymbol{Z}[X]$. We denote the square-norm of f by $\|f\|$, i.e., $\|f\|=\left(\sum_{i=0}^n |f_i|^2\right)^{1/2}$.

Lemma 24. *Let $\mathscr{T}_P$ be the set of all terms appearing in P. For each term T, we write c_T for its coefficient and set $D(T)=\max\{\deg_{x_1}(T),\ldots,\deg_{x_n}(T)\}$. Then the following M satisfies the condition at Step* 2.2:

$$M=\max\left\{\sum_{T\in\mathscr{T}_P}|c_T|\|f\|^{D(T)},\ 2[L:H]\right\}.$$

Proof. Let $\{i_1,\ldots,i_s\}$ be the set of all indices i such that $|\alpha_i|>1$. For each term $T=c_T x_1^{t_1}\cdots x_n^{t_n}$ appearing in P, $|\alpha_1|^{t_1}\cdots|\alpha_n|^{t_n}\leq|\alpha_{i_1}|^{D(T)}\cdots|\alpha_{i_s}|^{D(T)}$. By Landau's inequality [18, Theorem 3], $\prod_{i=1}^d \max\{1,|\alpha_i|\}\leq\|f\|$. From this, we get $|\alpha_{i_1}|^{D(T)}\cdots|\alpha_{i_s}|^{D(T)}\leq\|f\|^{D(T)}$ and $|T(\alpha_1,\ldots,\alpha_n)|\leq|c_T|\|f\|^{D(T)}$. □

Termination of the procedure. We assume that $p^{k+1}>(2M)^{[L:H]}$.

Lemma 25. *Suppose that $\mathscr{L}^L_{P,f}(y)$ is square-free and $\mathscr{L}^L_{P,f}(A) \equiv 0 \pmod{p^{K+1}}$ for an integer A with $|A| < M$. Then $\mathscr{L}^L_{P,f}(y)$ has A as a simple root modulo p^{k+1}.*

Proof. Let $m = [L:H]$ and $\mathscr{L}^L_{P,f}(y) = y^m + \ell_1 y^{m-1} + \cdots + \ell_m$. Since $(-1)^i \ell_i$ is the ith elementary symmetric function on roots of $\mathscr{L}^L_{P,f}(y)$, we have

$$|\ell_i| \leq {}_mC_i M^i.$$

Consider the differential $\mathrm{d}\mathscr{L}^L_{P,f}/\mathrm{d}y$. As $|A| < M$ and $2m < M$, we have

$$\begin{aligned} |\,\mathrm{d}\mathscr{L}^L_{P,f}/\mathrm{d}y(A)| &\leq mM^{m-1} + (m-1)|\ell_1|M^{m-2} + \cdots + |\ell_{m-1}| \\ &< mM^{m-1}(1 + {}_mC_1 + \cdots + {}_mC_{m-1}) \\ &< (2M)^m. \end{aligned}$$

Suppose that $\mathscr{L}^L_{P,f}(y) \equiv (y-A)^v h(y) \pmod{p^{k+1}}$ for $v \geq 2$ and for some polynomial $h(y)$ in $\boldsymbol{Z}[y]$. Then $\mathrm{d}\mathscr{L}^L_{P,f}/\mathrm{d}y(A) \equiv 0 \pmod{p^{k+1}}$. However, by the above estimate, as $p^{k+1} > (2M)^m$, we have $\mathrm{d}\mathscr{L}^L_{P,f}/\mathrm{d}y(A) = 0$. This contradicts the square-freeness of $\mathscr{L}^L_{P,f}$. □

By Lemma 25, if $\mathscr{L}^L_{P,f}$ is square-free, then the condition at Step (2.8) always holds. Thus, if we can find an H-invariant such that $\mathscr{L}^L_{P,f}$ is square-free, the whole procedure terminates.

Finding an H-invariant P was already discussed by several authors [3, 9, 13, 23]. Girstmair [13] proposed an algorithm for computing the lowest degree absolute H-invariant. Colin [9] showed that once we have an H-invariant P, we certainly generate an H-invariant P' such that $\mathscr{L}^L_{P',f}$ is square-free by *Tschirnhaus transformation* $P' = P(h(x_1), \ldots, h(x_n))$, where $h(x)$ is a polynomial of degree less than n. We will discuss this in Section 5.2.

5. On efficiency and practical efforts

To realize our method on real computers as a very practical one, the following two items are decisive: (1) an appropriate prime p, and (2) an invariant P for each subgroup H. In the sequent subsections, we discuss the effects of these to the total efficiency. We note that it is also important to find bounds on absolute values of invariants which are as small as possible.

Remark 26. To estimate the total efficiency of our method, we also have to analyze (1) the cost of finding all maximal subgroups up to conjugate in a given subgroup and (2) the bound of $\max\{[G_{i-1} : G_i]; 1 \leq i \leq r\}$, where $\{G_0 = S_n, G_1, \ldots, G_r = G_f\}$ is the computed sequence of maximal subgroups from S_n to the Galois group G_f of a given polynomial f.

5.1. Finding primes and lifting Gröbner bases

Let f be a square-free, monic integral polynomial f and p a prime number such that p does not divide the discriminant $d(f)$ of f. (By the estimate of $d(f)$, there are primes p such that $p = \mathrm{O}(n\log(n) + n\log(\|f\|))$.)

By using algebraic factorization over successive extensions, we compute the Gröbner basis $\bar{\mathscr{G}}$ of the splitting field $K_{\pi_p(f)}$ of $\pi_p(f)$ over $GF(p)$. Let $N_p = [K_{\pi_p(f)} : GF(p)]$ and $\pi_p(f) = \bar{f}_1 \cdots \bar{f}_r$ the factorization of $\pi_p(f)$ over $GF(p)$. As $N_p = \mathrm{lcm}(\deg(\bar{f}_1)\ldots,\deg(\bar{f}_r))$, we have a bound on N_p by [6]. By using [5, Section 5] for factorization we have the following. (For asymptotically faster algorithms, see [14].)

Lemma 27. *The Gröbner basis $\bar{\mathscr{G}}$ can be computed in $O(n^3N_p^3p\log(p)^2)$ binary operations and $N_p \leq \min\ \{\exp(\sqrt{6n\log(n)}, |G_f|\}$.*

Next, we lift $\bar{\mathscr{G}}$ to $\mathscr{G}^{(k)}$. Since all integer arithmetic is done modulo p^{k+1} in each step, the integer arithmetic can be done in $\mathrm{O}(k^2\log(p)^2)$. For the complexity of this step, we use the following estimate.

Lemma 28. *Let $\mathscr{R}$ be a local ring and $\mathscr{P}$ its maximal ideal. To lift all irreducible factors of a square-free polynomial of degree n over $\mathscr{R}/\mathscr{P}$ to their counterparts over $\mathscr{R}/\mathscr{P}^{k+1}$, it requires $\mathrm{O}(n^2k)$ arithmetic operations over $\mathscr{R}/\mathscr{P}^{k+1}$.*

Let$\bar{\mathscr{G}} = \{\bar{g}_1,\ldots,\bar{g}_n\}$. To lift each $\bar{g}_{i+1}$ to $g_{i+1}^{(k)}$, it requires $\mathrm{O}(n^2k)$ arithmetic operations over $\mathscr{R}_i = \boldsymbol{Q}_p[x_1,\ldots,x_i]/Id(g_1^{(\infty)},\ldots,g_i^{(\infty)})$. One arithmetic operation over $\mathscr{R}_i$ can be done in $\mathrm{O}(n_1^2\cdots n_i^2)$ arithmetic operations over $\boldsymbol{Z}$ modulo p^{k+1}, where $n_i = \deg_{x_i}(\bar{g}_i)$. Thus, we have the following estimate.

Lemma 29. *Lifting $\bar{\mathscr{G}}$ to $\mathscr{G}^{(k)}$ can be computed in $O(n^2N_p^2k^3\log(p)^2)$ binary operations.*

Thus, $\mathscr{G}^{(k)}$ can be computed in polynomial time in n, N_p, k and p. From this, it is better to choose a prime p for which N_p is as small as possible among a certain number of primes. In fact, the following p is desirable:

(i) $\pi_p(f)$ splits over $GF(p)$, i.e., $N_p = 1$. In [10] Darmon and Ford used such primes to show that G_f contains M_{11} or M_{12} for a certain polynomial f.

(ii) $\pi_p(f)$ splits over an extension field obtained by adding one root of an irreducible factor of $\pi_p(f)$ over $GF(p)$. That is, there is an irreducible factor $\bar{f}_i$ such that $K_{\pi_p(f)} \cong GF(p)[y]/Id(\bar{f}_i(y))$. In this case, $N_p = \deg(\bar{f}_i) \leq n$.

The Chebotarev density theorem suggests a certain probability that we succeed in finding such a prime. From the density theorem, we have the following:

Theorem 30 (cf. Pohst and Zassenhaus [21]). *For each positive integer A,*

$$|\{\sigma \in G_f \mid |\sigma| = A\}|/|G_f| \sim \lim_{m\to\infty} |\{p \mid N_p = A, p < m\}|/|\{p \mid p < m\}|.$$

Here, we call the ratio at the left side in Theorem 30 the *proportion* of primes p with $N_p = A$ and denote it by $\Pr(A)$. Then we have the following estimate.

(1) $\Pr(1) = 1/|G_f|$. Thus, it seems difficult to find such a prime p when $|G_f|$ is large.

(2) As $|G_f|$ divides $n!$, G_f has an element σ whose order is a prime number q and $q \leq n$. Then there are at least $[G_f : \mathrm{Cent}_{G_f}(\sigma)]$ elements of order q in G_f, where $\mathrm{Cent}_{G_f}(\sigma)$ denotes the centralizer of σ in G_f. Thus $\Pr(q) \geq 1/|\mathrm{Cent}_{G_f}(\sigma)|$. By considering the *cycle form* of σ (cf. [7, p. 9]), we have $|\mathrm{Cent}_{G_f}(\sigma)| \leq |\mathrm{Cent}_{S_n}(\sigma)| \leq (n-q)!q$ and so $\Pr(q) \geq 1/(n-q)!q$.

(3) When f is irreducible over $\boldsymbol{Q}$, G_f has a fixed-point free element σ of prime power order, i.e., the cycle form of σ consists of s_1 q^{e_1}-cycles, s_2 q^{e_2}-cycles,..., and s_r q^{e_r}-cycles for some prime q (see [8]). In this case, $|\mathrm{Cent}_{G_f}(\sigma)| \leq |\mathrm{Cent}_{S_n}(\sigma)| = s_1! \cdots s_r!$ $q^{s_1 e_1 + \cdots + s_r e_r}$. Letting q_0 be the smallest prime divisor of $|G_f|$, we have $|\mathrm{Cent}_{S_n}(\sigma)| \leq (n/q_0)! q_0^{n/q_0}$. Therefore, the proportion of primes p such that $N_p \leq n$ is at least $1/(n/q_0)!$ q_0^{n/q_0}. In particular, when n is prime, there is an element of order n in G_f and $\Pr(n) \geq 1/n$.

5.2. *Computation of invariants*

For a given subgroup H, we compute an H-invariant by existing methods [23, 13]. Here, we present estimates on sizes of H-invariants. Let $\mathrm{tdeg}(P)$ denote the total degree of P and $N_T(P)$ denote the number of terms in P. And let $C_T(P) = \max\{|c_T| \mid c_T$ is the coefficient of T appearing in $P\}$. We can see $\mathrm{tdeg}(P) \leq n(n-1)/2$.

Let P be the first computed L-relative H-invariant over $\boldsymbol{Z}$. If the condition at Step 2.8 fails, we have to replace P with another one. We generate H-invariants P' from P by Tschirnhaus transformations as follows:

(1) Let $\mathscr{V}_0 = \{\, v \in \boldsymbol{Z} \mid |v| \leq [L:H]([L:H]-1)\mathrm{tdeg}(P)/2\}$ and $\mathscr{V} = \mathscr{V}_0^n$.

(2) For each vector $V = (v_0, \ldots, v_{n-1})$ in $\mathscr{V}$, we set $F = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ and $P' = P(F(x_1), \ldots, F(x_n))$.

By [9, Proposition 9], we have the following:

Proposition 31. *There is a vector V in $\mathscr{V}$ such that $\mathscr{L}^L_{P',f}$ is square-free.*

The possibility that a random chosen V gives a square-free resolvent seems very high, however, we have only a worse bound $O([L:H]^{2n}\mathrm{tdeg}(P)^n)$ for the number of necessary transformations.

Remark 32. To avoid the explicit computation of P', we had better to compute $\mathrm{NF}_{\mathscr{G}(k)}$ $(F(x_i))$ for each i and evaluate P by those. In this case, we use the bound in Lemma 33 for M. Let P' be an H-invariant computed from P by a Tschirnhaus transformation which satisfies the condition at Step 2.8. Since $|\alpha| \leq \|f\| + 1$ for every root α of f, we have the following. (We also use the fact that $N_T(P)$ and $C_T(P)$ are less than $n!$.)

Lemma 33. *The absolute values of $\phi(P'^{\sigma})$'s are bounded by the following M:*

$$M = N_T(P) C_T(P) [L:H]^{2\,\mathrm{tdeg}(P)} \mathrm{tdeg}(P)^{\mathrm{tdeg}(P)} (2\|f\|)^{n\,\mathrm{tdeg}(P)},$$

Consequently, the bit length of the modulus p^{k+1} *is bounded by a polynomial in* n, $[L:H]$ *and* $\log(\|f\|)$.

5.3. Computation of splitting fields

By the new method we also obtain the following data: (a) the sequence $\{H_0 = S_n, H_1, \ldots, H_s = G_f\}$ of subgroups appearing in the computation of G_f, where H_i is a maximal subgroup of H_{i-1} for $1 \le i \le s$, (b) the H_i-invariant P_i used in the method and its integral value A_i for $1 \le i \le s$, and (c) the Gröbner basis $\mathcal{G}^{(k)}$ of the splitting ideal $\mathcal{M}^{(\infty)}$ modulo p^{k+1}. Here we give two usages of these data for computing the splitting field.

(1) By Corollary 9, the splitting ideal $\mathcal{M}$ over $\boldsymbol{Q}$ is constructed by

$$\mathcal{M} = \mathcal{M}_0 + Id(P_1 - A_1, \ldots, P_s - A_s).$$

Thus, we can compute the Gröbner basis with respect to any ordering by existing Gröbner basis algorithms.

(2) We can compute the Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_n\}$ of $\mathcal{M}$ with respect to the lexicographic order $<$ such that $x_1 < \cdots < x_n$ from $\bar{\mathcal{G}} = \pi_p(\mathcal{G}^{(k)})$ and G_f. (See the shape of g_i in Remark 2.) Here we give an outline. Let $\bar{\mathcal{G}} = \{\bar{g}_1, \ldots, \bar{g}_n\}$ and $\bar{\mathcal{M}} = Id(\bar{\mathcal{G}})$. Recall that G_f is already presented as a permutation group on X and $\mathrm{Aut}_{GF(p)}(GF(p)[X]/\bar{\mathcal{M}}) = G_{\pi_p(f)} \subset G_f$. Then, we know $\deg_{x_i}(g_i)$ for each i. Let $n_i = \deg_{x_i}(g_i)$. We compute $\pi_p(g_1), \ldots, \pi_p(g_n)$ by a *method of indeterminate coefficients* as follows: for $i = 1, \ldots, n$, we replace each coefficient of $\pi_p(g_i)$ with an indeterminate $a^{(i)}_{j_i,\ldots,j_1}$ as below:

$$\pi_p(g_i) = x_i^{n_i} + \sum_{j_i=0}^{n_i-1} \cdots \sum_{j_1=0}^{n_1-1} a^{(i)}_{j_i,\ldots,j_1} x_i^{j_i} \cdots x_1^{j_1}.$$

Then $\pi_p(g_i)(x_i^\sigma, \ldots, x_1^\sigma) = 0$ over $GF(p)[X]/\bar{\mathcal{M}}$ for every σ in G_f. This implies $\mathrm{NF}_{\bar{\mathcal{G}}}(\pi_p(g_i)(x_i^\sigma, \ldots, x_1^\sigma)) = 0$ for every σ in $L_i \backslash\backslash G_f$, where L_i is the point-wise stabilizer $\mathrm{Stab}_{G_f}(x_1) \cap \cdots \cap \mathrm{Stab}_{G_f}(x_i)$. We note $[G_f : L_i] = n_1 \cdots n_i$. Thus, for $\pi_p(g_i)$ we have a system of $n_1 \cdots n_i$ linear equations in $n_1 \cdots n_i$ variables.

Proposition 34. *Each system has a unique solution over* $GF(p)$. *Thus we can compute* $\pi_p(g_1), \ldots, \pi_p(g_n)$ *by solving the systems of linear equations.*

As a special case of [1], we know that $d(f)^C \mathcal{G} \subset \boldsymbol{Z}[X]$ for some integer C. (Cf. [16, p. 2]). By the same procedure as in Theorem 21, we can construct $\mathcal{G}$ from its image $\pi_p(\mathcal{G})$ by Hensel construction. From $\mathcal{G}^{(k)}$, we can also construct an approximation to $\mathcal{G}$ modulo p^{k+1} and then we can lift it to $\mathcal{G}$ by the Hensel construction.

Since the methods above use further information on the splitting fields, they are expected to be more efficient than direct computation of the splitting field by algebraic factorization when a given polynomial has large Galois group.

Table 1
Comparison the **new** method with galois in Maple (seconds)

	Group	*Galois*	*New*		Group	*Galois*	*New*
(7)	Z6	0.60	0.54	(8)	S3	0.63	0.57
(9)	D6	0.45	0.74	(10)	+A4	1.08	0.93
(11)	3.S3	2.13	0.79	(12)	2.A4	0.58	0.44
(13)	+S4/V4	0.60	0.85	(14)	S4/Z4	13.30	1.99
(15)	3^2.2^2	0.70	0.60	(16)	+3^2.4	0.58	0.74
(17)	2.S4	0.46	2.49	(18)	+PSL2(5)	0.58	2.19
(19)	3^2.D4	0.56	0.35	(20)	PGL2(5)	10.16	4.07
(23)	+Z7	0.45	0.85	(24)	D7	0.51	2.07
(25)	+F21	2.08	1.31	(26)	F42	2.28	8.80
(27)	+PSL3(2)	2.26	2.44				

Remark 35. From a preliminary experiment, the author found that sometimes it becomes very difficult to compute the Gröbner basis of $\mathscr{M}$ from the generating set shown in (1) directly by existing algorithms. In such a case, it seems very effective to eliminate indeterminates by resultant computation beforehand, and then compute the Gröbner basis of the *elimination ideal* of $\mathscr{M}$. Moreover, techniques on *basis-conversion* are also useful (see [4, 20]). By these techniques, we succeeded in computing a representation of the splitting field of the polynomial (27) in Table 2 (which is obtained by adding 4 roots) within 100 seconds on a Sun 4/20 workstation.

5.4. Experiment

Recent progress of the computer performance on integer operations encourages us to try polynomials with large degree, e.g., 15 or around. As the first step, we made a preliminary experiment on a real computer. We implemented the new method, on the computer algebra system Risa/Asir [19] for *irreducible* polynomials of degree 6 and 7. And we compared our implementation with *galois*, a known practical implementation, on Maple based on methods by McKay and his colleagues. We note that our implementation is not "complete" in the step of replacement of invariants and it assumes polynomials whose Galois groups are neither S_n nor A_n. The reason why the degree of the polynomials are chosen as 6 and 7 is two-fold: *galois* of Maple can handle polynomials up to degree 7 and much preparation time is required for computing tables to deal with polynomials of higher degree. We found that the new method is comparable to *galois* for several examples. Although the comparison was made for small number of polynomials and our implementation is not a complete one, the author is pleased with the quality and ability of the method.

Table 1 shows the comparison with *galois* for polynomials listed in Table 2 used as examples in [2]. The timings were measured on a Sun 4/20 with 64 Mbyte memory. For three key parts, choice of primes, invariants, and the semi-lattice of subgroups of S_n, we used the following strategy:

Table 2

Sample polynomials	
(7) x^6+x^3+1	(8) $x^6+2x^3+9x^2-6x+2$
(9) x^6-3	(10) $x^6+9x^4-4x^2-4$
(11) x^6+x^3+7	(12) x^6-3x^4+1
(13) x^6+x^4-9	(14) x^6+6x^2+4
(15) x^6-2x^3-2	(16) $x^6+6x^4+2x^3+9x^2+6x-4$
(17) x^6+x^4-8	(18) $x^6-9x^3+6x^2+9x+2$
(19) $x^6+x^4-x^2+5x-5$	(20) $x^6+10x^5+55x^4+140x^3+175x^2-3019x+25$
(23) $x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$	(24) $x^7+7x^3+7x^2+7x-1$
(25) $x^7-14x^5+56x^3-56x+22$	(26) x^7-2
(27) x^7-7x+3	

Primes: Let $f(x)$ be the given polynomial. Since $\deg(f)=6$ or 7, its Galois group G_f is small except S_7, A_7. We choose a prime p such that $\pi_p(f)$ splits over $GF(p)$. In this case, similarly to Darmon and Ford in [10], we can use an ordinary Hensel construction procedure for lifting each linear factor of $\pi_p(f)$. As mentioned in Section 5.1, the proportion of such primes among all primes is close to the ratio $1/|G_f|$, so we could find such a prime p quickly for these examples.

Invariants: We just used the results given in [23, 13]. As mentioned before, we did not implement the step of replacement of invariants completely. (We used polynomials with degree less than 3 for Tschirnhaus transformation).

Subgroups: Similarly, we did not compute maximal (transitive) subgroups; instead, we used the semi-lattices given by [23].

5.5. *Further remark on modular technique*

A similar technique using extension fields of p-adic number fields is applied to compute subfields in [15]. By the subfield computation, we can determine whether the Galois group G_f of a given polynomial f has an imprimitive block system and we can find an imprimitive block very efficiently if G_f has. Since imprimitive blocks give very useful information on the Galois group, we can incorporate this procedure into the method for Galois groups effectively with keeping advantage of the modular technique.

Acknowledgements

The work here was partly done during the author's stay at RISC-Linz. The author would like to thank Prof. Buchberger for his support at RISC-Linz, Prof. McKay for helpful comments and references [10, 15, 17] and his colleagues Mr. Noro and Mr. Anai for their support on experiments. Also, the author would like to mention that in developing main ideas of the paper, he was inspired by Pohst and Zassenhaus [21] which suggested evaluating invariants over $GF(p)$ or its extension.

References

[1] J.A. Abbott, On the factorisation of polynomials over algebraic fields, Ph.D. Thesis, School of Math. Sci., University of Bath, 1989.

[2] H. Anai, M. Noro and K. Yokoyama, Computation of the splitting fields and the Galois groups of polynomials, in: L. González-Vega and T. Recio, eds., Algorithms in Algebraic Geometry and Applications (Birkhäuser, Basel, 1996) 29–50.

[3] J.-M. Arnaudiès and A. Valibouze, Résolvantes de Lagrange, Rapport LITP 93.61, 1993.

[4] T. Becker and V. Weispfenning, Gröbner Bases (Springer, New York, 1993).

[5] E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comput. 24 (1970) 713–735.

[6] J. Berstel and M. Mignotte, Deux propriétés décidables des suites récurrentes linéaires, Bull. Soc. Math. France 104 (1976) 175–184.

[7] G. Butler, Fundamental Algorithms for Permutation Groups, Lecture Notes in Comp. Sci., Vol. 559 (Springer, New York, 1991).

[8] P.J. Cameron, Some open problems on permutation groups, in: M.W. Liebeck and J. Saxl, eds., Groups, Combinatorics and Geometry (Cambridge Univ. Press, Cambridge, 1992) 340–350.

[9] A. Colin, Formal computation of Galois groups with relative resolvents, in: Proc. AAECC-11, Lecture Notes in Comp. Sci., Vol. 948 (Springer, New York, 1995) 169–182.

[10] H. Darmon and D. Ford, Computational verification of M_{11} and M_{12} as Galois groups over $\boldsymbol{Q}$, Commun. Algebra 17 (1989) 2941–2943.

[11] Y. Eichenlaub and M. Olivier, Computation of Galois groups for polynomials with degree up to eleven, preprint, 1994.

[12] D.J. Ford and J. McKay, Computation of Galois groups from polynomials over the rationals, in: Computer Algebra, Lecture Notes in Pure Appl. Math., Vol. 113 (Springer, New York, 1989) 145–150.

[13] K. Girstmair, On invariant polynomials and their application in field theory, Math. Comput. 48 (1987) 781–797.

[14] E. Kaltofen, Polynomial factorization 1987–1991, in: LATIN'92, Lecture Notes in Comput. Sci., Vol. 583 (Springer, New York, 1992) 294–313.

[15] J. Klüners and M. Pohst, On computing subfields, preprint, 1996.

[16] L. Langemyr, Algorithms for a multiple algebraic extension II, in: Proc. AAECC-9, Lecture Notes in Comp. Sci., Vol. 539 (Springer, New York, 1991) 224–233.

[17] T. Mattman and J. McKay, Computation of Galois groups over function fields, Math. Comput. (1996) to appear.

[18] M. Mignotte, Some useful bounds, in: Computer Algebra (Springer, Wien, 1982) 259–263.

[19] M. Noro and T. Takeshima, Risa/Asir–a computer algebra system, in: Proc. ISSAC'92 (ACM Press, New York, 1992) 387–396.

[20] M. Noro and K. Yokoyama, New methods for the change-of-ordering in Gröbner basis computation, Research Report ISIS-RR-95-8E, 1995.

[21] M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory (Cambridge Univ. Press, Cambridge, 1989).

[22] L. Soicher and J. McKay, Computing Galois groups over the rationals, J. Number Theory 20 (1985) 273–281.

[23] R.P. Stauduhar, The determination of Galois groups, Math. Comput. 27 (1973) 981–996.

[24] N. Tschbotarev and H. Schwerdtfeger, Grundzüge des Galois'schen Theorie (P. Noodhoff, Groningen, 1950).

[25] A. Valibouze, Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems, in: Proc. AAECC-11, Lecture Notes in Comp. Sci., Vol. 948 (1995) 456–468.

[26] P.J. Weinberger and L.P. Rothschild, Factoring polynomials over algebraic number fields, ACM Trans. Math. Software 2 (1976) 335–350.