ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 23–40

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Lagrange resolvents

Jean-Marie Arnaudiès[a,1], Annick Valibouze[b,*,1,2]

[a] *Institut de Mathématiques, Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05, France*
[b] *LITP, Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05, France*

Abstract

This paper is devoted to an investigation of the notion of Lagrange's resolvent and its connections with Galois theory. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 11Y40

1. Introduction

Among the first questions encountered in Galois theory, the problem of computing the Galois group of a given polynomial (e.g., of the splitting field of this polynomial, relatively to the base field) is quite natural. We will call it the *direct Galois problem*. Early mathematicians, concerned with the so-called *Galois* theory, created the concept of *resolvent*, a very suitable notion in the Galois direct problem. In fact, resolvents and Galois groups were discovered simultaneously, essentially by Lagrange, whose papers on algebraic equations really contain reasonings about groups, although Lagrange did not clearly define them. In these papers, the correspondence between groups and resolvents is also displayed, rather more deeply than by Galois himself (the main contribution of Galois seems related to groups, not to resolvents; he certainly knew Lagrange's work, but did not have enough time to develop all ideas arising from this knowledge). During the 19th century, no really new ideas about algebraic equations were found after those of Lagrange, Abel and Galois, and in most papers or monographs, Galois theory was developed using resolvents and nothing else. In the well-known works of

[*] Corresponding author. E-mail: avb@medicis.polytechnique.fr. WWW http://medicis.polytechnique.fr/medicis/projetGalois.
[1] Projet Galois of the GDR de Calcul Formel MEDICIS.
[2] GAGE, Centre de Calcul Formel de l'Ecole Polytechnique.

PII S0022-4049(97)00003-0

Kronecker, Vogt, Weber, Jordan and others, attempts, very similar to one another, to determine the Galois group of a polynomial are found: one begins with a resolvent, chosen above all according to its ease of determination; whenever this resolvent has a root in the base field, by what all these authors call *the main Galois theorem on resolvents*, the Galois group will be contained in the group of this resolvent. If not, one adds a root of the resolvent to the base field, and so on. What is obtained in this manner is a Jordan–Hölder sequence of the Galois group, but where only the successive factor groups are known. Moreover, none of these authors points out the case of multiple roots in a resolvent, a circumstance under which the *main Galois theorem* becomes false (note that in Lagrange's original papers, this case is considered, and Lagrange not only says that then the method fails; but he suggests some ideas to overcome this obstacle; see [11]).

The first author who really considered the set of all resolvents of a given polynomial and looked at the structure of this set within Galois groups was Berwick. In fact, he uses parts of what we call *partition tables* to deduce the Galois group from certain configurations of the resolvent factorizations over the base field (see [3]). After him, Soicher, Foulkes, Stauduhar, McKay and others investigated this method, obtaining significant results. For example, it can be found, in several of their works, that the factorization of a single separable resolvent suffices to deduce the Galois group of an irreducible polynomial of degree 7. Soicher and McKay calculate partial partition tables associated to *linear resolvents*, thus deducing Galois groups from this factorization of resolvents in many cases up to degree 11 (see [5, 8, 12, 14], etc.).

In this paper, we present our main idea for improving the use of resolvents in the direct Galois problem for a polynomial f. Instead of starting with resolvents, we consider the set of all subgroups of the symmetric group $\mathfrak{S}_n$ (n = degree of f). We associate to it a square matrix whose coefficients are *partitions* of integers (here, we mean the word *partition* in its *combinatorial* sense, not in its *set-theoretical* sense). These partitions are related to the different pairs of conjugacy classes of the subgroups of $\mathfrak{S}_n$. We call this matrix the *partition matrix* of $\mathfrak{S}_n$. Its rows and columns both correspond to the conjugacy classes of subgroups of $\mathfrak{S}_n$, but not in the same manner: the row conjugacy classes of groups must be viewed as *candidates* for being the conjugacy class of the sought for Galois group of f, and the column conjugacy classes of groups, as *test* conjugacy classes. To each test conjugacy class, we associate a resolvent of f; factoring the latter over the base field, we get a certain partition. We show that the family of partitions obtained by taking successively all the test conjugacy classes, builds one, and exactly one, row of the partition matrix (see Theorem 14). Thus, the direct Galois problem for f amounts to recognizing this row, i.e. to effectively factorize all the resolvents associated to test groups. This seems to be a tremendous task; fortunately, one needs not compute all these resolvents. In many cases of interest, only a few of them, associated to test groups of low index in $\mathfrak{S}_n$, are sufficient for our purpose. Moreover, when these resolvents are not irreducible (as happens almost systematically when the sought for Galois group has high index in $\mathfrak{S}_n$), one needs not the whole resolvent, but only some of its factors (see [2]). So, our method allows us to compute Galois groups of separable (not necessarily irreducible) polynomials in many cases up to degree 11: in 1993, we also gave a complete algorithm for separable polynomials up to degree 7, and for irreducible polynomials of degree 8, 9 and 11; we also gave an algorithm which covers partially the case of irreducible polynomials of degree 10 (see also [15]).

The idea of a partition matrix can be extended to a general finite reference group as well as $\mathfrak{S}_n$. This leads to a generalization of our method to the so-called *relative* resolvents, the ones considered above being called *absolute* resolvents (see Section 4).

Finally, the partition matrix can also be a powerful theoretical tool, not only a numerical one. As examples, we give a general theorem relating some resolvents, which are very easy to compute, to cyclic or metacyclic Galois groups (see [2]), and we develop a complete method for the Galois group of a polynomial of fifth degree having general coefficients (see [6]); the parallel method for polynomial of fourth degree can be found in [1].

Contents of the paper: Section 2 is devoted to the concept of Lagrange resolvent; Section 3 introduces the partition matrix, with statements and proofs of the main results mentioned above; Section 4 gives an extension to relative resolvents; and Section 5 contains some original theoretical results on resolvents.

2. The concept of resolvent

2.1. Permutation representations

Let K be a commutative field and let E be a Galois extension of K. For each polynomial $f \in K[X]$ normal over K, the Galois group $\mathrm{Gal}\,(E/K)$ admits a natural representation in the permutation group of the root set of f. Thus, it will be useful to recall some elementary facts concerning permutation representations. For details, see [4].

Notation. Let $\mathscr{C}$ be a conjugacy class of subgroups of a finite group G. We will denote $I_{\mathscr{C}}$ the subgroup $\bigcap_{H\in\mathscr{C}} H$ of G. Then $I_{\mathscr{C}}$ is a normal subgroup of G, notation $I_{\mathscr{C}} \lhd G$. The class $\mathscr{C}$ will be said to be *reduced* if and only if $I_{\mathscr{C}} = \{e_G\}$. Now, let E be a finite non-empty set. One defines a *permutation representation* of G in E as a group morphism: $\Psi : G \longrightarrow \mathfrak{S}_E$. The integer $N = \mathrm{card}\,(E)$ is called the *degree* of Ψ. The representation Ψ is said *faithful* if and only if Ψ is injective, *transitive* if and only if the G-set E defined by Ψ has but one orbit, and *primitive* if and only if the corresponding G-set is primitive. When Ψ is transitive, the set $\{\mathrm{Stab}_G(x)\}_{x\in E}$ is a conjugacy class of subgroups of G, which will be said *associated* with Ψ.

Two permutation representations $\Psi : G \longrightarrow \mathfrak{S}_E$ and $\Phi : G \longrightarrow \mathfrak{S}_F$ are called *equivalent* if and only if there is a bijection $\Theta : E \longrightarrow F$ such that $\Psi(G) = \Theta^{-1} \circ \Phi(G) \circ \Theta$ for all $g \in G$. In case Ψ and Φ are equivalent, then $\mathrm{Ker}\,(\Phi) = \mathrm{Ker}\,(\Psi)$, the conjugacy classes of subgroups associated with them as above are the same; thus Φ and Ψ are both faithful or not, and both transitive or not.

Clearly, a permutation representation of degree N of G is equivalent to a permutation representation of G in $[\![1, N]\!]$. The latter will be called a *symmetric* representation of G (of degree N).

2.2. *Transitive permutation representations*

Let $\Psi : G \to \mathfrak{S}_E$ a transitive permutation representation of the finite group G. Denote by $\mathscr{C}_\Psi$ the associated class: it is reduced if and only if Ψ is faithful. Now, choose any $x_0 \in E$; put $H_0 = \mathrm{Stab}_G(x_0)$. For every element $x \in E$, the set $\Theta(x) = \{g \in G \mid \Psi(g)(x_0) = x\}$ is a left coset of G mod H_0. The map Θ of E into the set (G/H_0) is one-to-one; it is readily seen that Θ establishes an equivalence between Ψ and the permutation representation Φ of G in $\mathfrak{S}_{(G/H_0)}$ defined by the left translations of G. The following well-known theorem is easy to check:

Theorem 1. *Let G be a finite group; let E be a non-empty finite set; put $N = \mathrm{card}\,(E)$. The mapping sending each equivalence class Γ of transitive permutation representations of G in E to its associated conjugacy class of subgroups $\mathscr{C}_\Gamma$ defines a bijection of the set of these representations onto the set of those conjugacy classes of subgroups of G all elements of which have index N in G. This bijection associates reduced classes to faithful representations. The class $\{\{e_G\}\}$ corresponds to the set of regular representations.*

2.3. *Permutation representations and splitting fields*

For the remainder of the paper, we will denote by k a fixed commutative field, and we will choose once and for all an algebraic closure $\overline{k}$ of k. To each polynomial $f \in k[X]$, there corresponds the splitting field E_f of f over k, i.e. the k-algebra generated in $\overline{k}$ by the root set of f. Now consider a *separable* non-constant monic polynomial $f \in k[X]$, of degree n, together with an ordering $\rho_1, \dots, \rho_n$ of its roots in $\overline{k}$. Then we obtain a symmetric representation of degree n of $\mathrm{Gal}\,(E_f/k)$:

$$\mathrm{Gal}\,(E_f/k) \longrightarrow \mathfrak{S}_n, \quad \sigma \longmapsto s_\sigma \tag{1}$$

where $s_\sigma(\rho_i) = \rho_{s_\sigma(i)}$ for all i ($1 \le i \le n$). This representation will be called *associated* with the given ordering (ρ_i) of the root set of f. It is faithful; it is transitive if and only if f is irreducible.

Let $t \in \mathfrak{S}_n$. Put $\rho'_i = \rho_{t^{-1}(i)}$ for all i. The symmetric representation associated with the new ordering (ρ'_i) is equivalent to the representation (1), for it is given by the map: $\sigma \mapsto s'_\sigma = t s_\sigma t^{-1}$. When k is infinite, it is well-known that for each Galois extension E of k, any faithful symmetric representation of $\mathrm{Gal}\,(E/k)$ is obtainable as the representation associated with an ordering of the root set in $\overline{k}$ of a suitable separable polynomial $f \in k[X]$ (see [2]). Note that the regular left representation of G corresponds to the case where f is the minimal polynomial of any primitive element of E over k.

2.4. *Generic resolvents*

Let n be a fixed natural integer; let $X_1,\dots,X_n$ be indeterminates over $\bar{k}$. Denote by $\mathscr{F}$ the field $k(X_1,\dots,X_n)$, by $\mathscr{A}$ the ring $k[X_1,\dots,X_n]$, by $\sigma_1,\dots,\sigma_n$ the elementary symmetric polynomials in the variables $X_1,\dots,X_n$, by $\mathscr{S}$ the ring $k[\sigma_1,\dots,\sigma_n]$, and by $\mathscr{K}$ the field $k(\sigma_1,\dots,\sigma_n)$. This notation will be used throughout the remainder of this paper. $\mathscr{F}$ is the splitting field over $\mathscr{K}$ of $F(T) = T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n\sigma_n = \prod_{i=1}^n (T - X_i) \in \mathscr{S}[T]$; so, $\mathscr{F}$ is a Galois extension of $\mathscr{K}$; the symmetric representation associated with the ordering $X_1,\dots,X_n$ of the roots of F is a group isomorphism: $\mathrm{Gal}(\mathscr{F}/\mathscr{K}) \to \mathfrak{S}_n$. It will be convenient to *identify* the groups $\mathrm{Gal}(\mathscr{F}/\mathscr{K})$ and $\mathfrak{S}_n$ by means of this isomorphism. Thus, for all $\sigma \in \mathfrak{S}_n$ and $f = f(X_1,\dots,X_n) \in \mathscr{F}$, the image of f under the action of σ is $f(X_{\sigma(1)},\dots,X_{\sigma(n)})$: it will be denoted by $\sigma \bigstar f$.

To each subgroup H of $\mathfrak{S}_n$, we will designate by $\mathrm{Inv}(H)$ the field of H-invariants in $\mathscr{F}$. Then $\mathrm{Inv}(H)$ is separable over $\mathscr{K}$, $\mathscr{F}$ is a Galois extension of $\mathrm{Inv}(H)$, and $\mathrm{Gal}(\mathscr{F}/\mathrm{Inv}(H)) = H$. The integral closure $\mathscr{A}_H$ of $\mathscr{S}$ in $\mathrm{Inv}(H)$ is $\mathscr{A} \cap \mathrm{Inv}(H)$. The k-algebra $\mathscr{A}_H$ is finitely generated; it is an integrally closed, Noetherian ring; it follows that $\mathscr{A}_H$ is a finitely generated $\mathscr{S}$-module. In other words, $(\sigma_1,\dots,\sigma_n)$ is a *homogeneous system of parameters* of the k-algebra $\mathscr{A}_H$ in the sense of [13]. Moreover, $\mathrm{Inv}(H)$ is the field of fractions of $\mathscr{A}_H$; more precisely, $\mathscr{A}_H\,[1/\mathscr{S}] = \mathrm{Inv}(H)$.

Definition 2. Under the above conditions, we will call primitive invariant of H any polynomial $\Psi \in \mathscr{A}_H$ which is a primitive element of the extension field $\mathrm{Inv}(H)$ of $\mathscr{K}$. Such a Ψ will be called *homogeneous* whenever it is an homogeneous polynomial in the X_i's. The minimal polynomial over $\mathscr{K}$ of a primitive invariant Ψ of H will be called the (generic) Lagrange resolvent of H associated to Ψ. We will denote it by $\mathscr{L}_\Psi$.

The next theorem, due to Lagrange, is both of mathematical and of historical interest.

Theorem 3. *Let Ψ be a primitive invariant of a subgroup H of $\mathfrak{S}_n$. Denote by Δ_Ψ the discriminant of the generic resolvent $\mathscr{L}_\Psi$. Then $\mathscr{A}_H \subset (1/\Delta_\Psi)\mathscr{S}[\Psi]$.*

Proof. We give the original proof of Lagrange, which even nowadays remains the best. Let e be the index $[\mathfrak{S}_n : H]$. Choose a left transversal $\{t_i\}_{1\le i\le e}$ of $\mathfrak{S}_n \bmod H$, such that $t_1 = \mathrm{Id}_{\mathfrak{S}_n}$. Put $\Psi_i = t_i \bigstar \Psi$ (hence, $\Psi_1 = \Psi$). Denoting by X an indeterminate over $\mathscr{F}$, we have

$$\mathscr{L}_\Psi(X) = \prod_{i=1}^{e}(X - \Psi_i) = X^e - C_1X^{e-1} + \cdots + (-1)^e C_e \in \mathscr{S}[X]. \tag{2}$$

Take any $g \in \mathscr{A}_H$. Put $g_j = t_j \bigstar g$. For $m \in [\![0, e-1]\!]$, define

$$h_m = \sum_{j=1}^{e} g_j \Psi_j^m = \sum_{j=1}^{e} t_j \bigstar (g\Psi^m)\ . \tag{3}$$

Clearly, $h_m \in \mathscr{S}$. We may consider Eqs. (3) as a linear system in the g_j's. Of course, this is a Cramer system; by solving it, we especially obtain

$$g_1 = \frac{1}{\delta_\Psi}\mathscr{D}, \tag{4}$$

where δ_Ψ is the Vandermonde determinant with respect to $\Psi_1, \dots, \Psi_e$, i.e., $\delta_\Psi = \prod_{1 \le i < j \le e}(\Psi_j - \Psi_i)$, and

$$\mathscr{D} = \begin{vmatrix} h_0 & 1 & \cdots & 1 \\ h_1 & \Psi_2 & \cdots & \Psi_e \\ \vdots & \vdots & & \vdots \\ h_{e-1} & \Psi_2^{e-1} & \cdots & \Psi_e^{e-1} \end{vmatrix}.$$

Due to $\delta_\Psi^2 = \Delta_\Psi$, the latter can be written as

$$g = \frac{1}{\Delta_\Psi}\mathscr{E} \quad \text{where } \mathscr{E} = \delta_\Psi \mathscr{D}. \tag{5}$$

Now, we shall prove that $\mathscr{E} \in \mathscr{S}[\Psi]$. To this aim, note that $\mathscr{E} = E(\Psi_1, \dots, \Psi_e)$ for a suitable polynomial $E \in \mathscr{S}[\Psi][T_2, \dots, T_e]$, symmetric in the variables $T_2, \dots, T_e$. By the main theorem on symmetric functions, denoting $S_1, \dots, S_{e-1}$ the elementary symmetric polynomials in $\Psi_2, \dots, \Psi_e$, we get a polynomial $F \in \mathscr{S}[\Psi][Y_1, \dots, Y_{e-1}]$ such that $E(\Psi_2, \dots, \Psi_e) = F(S_1, \dots, S_{e-1})$. Now $\prod_{i=2}^{e}(X - \Psi_i) = \mathscr{L}_\Psi(X)/(X - \Psi) = X^{e-1} + (\Psi - C_1)X^{e-2} + \cdots \in \mathscr{S}[\Psi][X]$. Hence, $S_j \in \mathscr{S}[\Psi]$ for all $j \in [\![1, e-1]\!]$. We deduce $\mathscr{E} = F(S_1, \dots, S_{e-1}) \in \mathscr{S}[\Psi]$, so by taking (5) into account, $g \in \frac{1}{\Delta_\Psi}\mathscr{S}[\Psi]$. □

Theorem 4. *Assume k is of zero characteristic. For each subgroup H of $\mathfrak{S}_n$, the $\mathscr{S}$-module $\mathscr{A}_H$ is finitely generated, and free of rank $e = [\mathfrak{S}_n : H]$.*

Proof. The freedom of the finitely generated $\mathscr{S}$-module $\mathscr{A}_H$ comes from the above noticed property of $(\sigma_1, \dots, \sigma_n)$ being a homogeneous system of parameters (see [13]). Obviously, the rank r of this module is given by $r = \dim_{\mathscr{K}}(\mathscr{K} \bigotimes_{\mathscr{S}} \mathscr{A}_H)$. But $\mathrm{Inv}(H) = \mathscr{A}_H[1/\mathscr{S}] \cong \mathscr{K} \bigotimes_{\mathscr{S}} \mathscr{A}_H$. By Galois theory, we deduce $r = \dim_{\mathscr{K}}(\mathrm{Inv}(H)) = [\mathfrak{S}_n : H]$, as expected. □

Under the assumptions of the above theorem, an effective construction of a basis for the $\mathscr{S}$-module $\mathscr{A}_H$ can be given (see [2]). The field k being still assumed infinite (of any characteristic), it can be shown that there exist *homogeneous* elements of $\mathscr{A}_H$ which are primitive over $\mathscr{K}$ for the extension field $\mathrm{Inv}(H)$ (see [2, p. 11]).

2.5. Specialized resolvents

In this section, we fix a *separable* monic polynomial $f = X^n - c_1X^{n-1} + \cdots + (-1)^n c_n \in k[X]$, of degree $n \ge 1$, and we denote by E its splitting field in $\bar{k}$. The set of roots $\mathscr{R}_f$ of f will be ordered once and for all: $\mathscr{R}_f = \{\rho_1, \dots, \rho_n\}$. In order to abridge notations, we denote the specialization morphism

$$\mathscr{A} \to \overline{k}, \qquad \varphi = \varphi(X_1, \dots, X_n) \mapsto \varphi(\rho_1, \dots, \rho_n)$$

by $\varphi \mapsto \widetilde{\varphi}$. Obviously, $\widetilde{\sigma_i} = c_i$ for $1 \le i \le n$.

Definition 5. Let Ψ be a primitive invariant of a subgroup H of $\mathfrak{S}_n$. The polynomial obtained by substituting the above c_i's to the σ_i's in the generic resolvent $\mathscr{L}_\Psi$ will be called the *(H, Ψ)-resolvent of f*; we will denote it by $\mathscr{L}_{\Psi,f}$. The invariant Ψ will be said to be *f-separable* if and only if $\mathscr{L}_{\Psi,f}$ is separable.

As separable resolvents are the easiest ones to deal with, we must make sure to have at our disposal a whole crowd of them:

Theorem 6. *Assume k is infinite. Let A be a subring of k whose quotient field is k. Then there exists a primitive homogeneous f-separable invariant Ψ of H belonging to $A[X_1, \dots, X_n]$.*

Proof. Let $\mathscr{H}$ be the set of left cosets $\mathfrak{S}_n/H$. Take n indeterminates $U_1, \dots, U_n$ over $\mathscr{F}$. As the ρ_i's are distinct, the $n!$ elements $(\sum_{i=1}^n U_i\rho_{s(i)})-1, (s \in \mathfrak{S}_n)$ of $k[U_1, \dots, U_n]$ are mutually coprime. Hence, defining $\varphi_C \in k[U_1, \dots, U_n]$ for $C \in \mathscr{H}$ by

$$\varphi_C = \prod_{s \in C} \Big((\sum_{i=1}^{n} U_i \rho_{s(i)}) - 1 \Big), \tag{6}$$

we find that these φ_C's are mutually coprime too; a fortiori, they are distinct. As A is infinite, we may choose $(u_1, \dots, u_n) \in A^n$ such that the mapping $\mathscr{H} \to k[U_1, \dots, U_n]$, $C \mapsto \varphi_C(u_1, \dots, u_n)$ is injective. Then put

$$\Psi = \prod_{s \in H} \Big((\sum_{i=1}^{n} u_i X_{s(i)}) - 1 \Big). \tag{7}$$

We have $\Psi \in \mathrm{Inv}(H) \cap A[X_1, \dots, X_n]$. The conjugates of Ψ in $\mathscr{F}$ over $\mathscr{K}$ are the various $\Psi_C = \prod_{s \in C}((\sum_{i=1}^n u_i X_{s(i)}) - 1)$ as C describes $\mathscr{H}$. (Note that $\Psi = \Psi_H$.) By the choice of the u_i's, these conjugates are all distinct. So, Ψ is a primitive invariant for H. But clearly

$$\mathscr{L}_{\Psi,f}(X) = \prod_{C \in \mathscr{H}} \Big(X - \Psi_C(\rho_1, \dots, \rho_n) \Big), \tag{8}$$

hence the polynomial $\mathscr{L}_{\Psi,f}$ is separable. In order to obtain a *homogeneous* primitive invariant, take a new indeterminate λ over $\mathscr{F}$. For $C \in \mathscr{H}$, denote by $(\Psi_C)_\lambda$ the $\lambda\sigma_1$-homogenized polynomial

$$(\lambda\sigma_1)^d \Psi_C \left(\frac{X_1}{\lambda\sigma_1}, \dots, \frac{X_n}{\lambda\sigma_1} \right),$$

where d designates the $(X_1,\dots,X_n)$-degree of Ψ_C. Put

$$\mathscr{P}_\lambda(X) = \prod_{C\in\mathscr{H}} \Big(X-(\Psi_C)_\lambda\Big), \tag{9}$$

let $\mathscr{D}(\lambda)$ be the X-discriminant of $\mathscr{P}_\lambda(X)$ and $D(\lambda)$ the element of $A[\lambda]$ obtained by specializing the σ_i's to the c_i's in $\mathscr{D}(\lambda)$. Then $D(1/\sigma_1) \neq 0$, because here we have nothing but the discriminant of $\mathscr{P}_{1/\sigma_1}(X) = \mathscr{L}_{\Psi,f}(X)$. So, $D(\lambda) \neq 0$. As A is infinite, we can now choose $a \in A$ such that $D(a) \neq 0$. Let $\Theta_C = (\Psi_C)_\lambda|_{\lambda \leadsto a}$ and $\Theta = \Theta_H$. Clearly, $\Theta \in \mathrm{Inv}(H)\cap A[X_1,\dots,X_n]$; Θ is homogeneous of degree card(H) in the X_i's. The conjugates of Θ over $\mathscr{K}$ are the Θ_C's. Finally, let $\theta_C \in k$ obtained by substitution of the ρ_i's to the X_i's in Θ_C, i.e. $\theta_C = \widetilde{\Theta_C}$. The polynomial $\mathscr{L}_{\Theta,f}(X) = \prod_{C\in\mathscr{H}}(X-\theta_C)$ has discriminant $D(a) \neq 0$. Therefore, on the one hand, the Θ_C's are all distinct, so Θ is a primitive invariant of H, and on the other hand, $\mathscr{L}_{\Theta,f}$ is separable, i.e. Θ is f-separable. □

Theorem 7. *Let k be infinite. Give A as in Theorem 6. Let Ψ be a primitive f-separable invariant of a subgroup H of $\mathfrak{S}_n$. Assume $n \geq 5$ and $H \notin \{\mathfrak{A}_n, \mathfrak{S}_n\}$. Then the splitting field over k of $\mathscr{L}_{\Psi,f}$ is E, that of f.*

Proof. Let $\Psi_1,\dots,\Psi_e$ be the conjugates of Ψ over $\mathscr{K}$, with $\Psi = \Psi_1$. Put $\widetilde{\Psi}_i = \Psi_i(\rho_1,\dots,\rho_n)$. Choose elements $a_1,\dots,a_e$ of A such that the $e!$ elements $\lambda_s = \sum_{i=1}^e a_i \widetilde{\Psi}_{s(i)}$ $(s \in \mathfrak{S}_e)$ be distinct (their existence comes readily from the hypotheses). The natural action of $\mathfrak{S}_n = \mathrm{Gal}(\mathscr{F}/\mathscr{K})$ is transitive. As $n \geq 5$, the only normal proper subgroups of $\mathfrak{S}_n$ are $\{\mathrm{Id}\}$ and $\mathfrak{A}_n$. As $e \geq 3$, the above action is faithful, which implies: $\mathscr{K}[\Psi_1,\dots,\Psi_e] = \mathscr{F}$.

Let Γ_n be the image of $\mathfrak{S}_n$ in $\mathfrak{S}_e$ resulting from this representation. The $n!$ elements $\sum_{i=1}^e a_i\Psi_{s(i)}$ $(s \in \Gamma_n)$ of $\mathscr{F}$ are obviously distinct; therefore, $\Phi = \sum_{i=1}^e a_i\Psi_i$ is a primitive element of $\mathscr{F}$ over $\mathscr{K}$. Apply Theorem 3 with $H = \{\mathrm{Id}\}$ and with the primitive invariant Φ of H. Here $\mathscr{A}_H = \mathscr{A}$; thus, $\mathscr{A} \subset (1/\Delta_\Phi)\ \mathscr{S}[\Phi]$, where Δ_Φ is the X-discriminant of the polynomial $\prod_{s\in\Gamma_n}(X - \sum_{i=1}^e a_i\Psi_{s(i)})$. From $\mathscr{S}[\Phi] \subset \mathscr{S}[\Psi_1,\dots,\Psi_e]$, we infer

$$\mathscr{A} \subset \frac{1}{\Delta_\Phi}\mathscr{S}[\Psi_1,\dots,\Psi_e], \quad \text{i.e.} \quad \Delta_\Phi\mathscr{A} \subset \mathscr{S}[\Psi_1,\dots,\Psi_e]. \tag{10}$$

Set

$$\widetilde{\Delta}_\Phi = \Delta_\Phi(\rho_1,\dots,\rho_n)\ \left(= (-1)^{n!(n!-1)/2} \prod_{s\in\Gamma_n, t\in\Gamma_n, s\neq t} (\lambda_s - \lambda_t)\right).$$

Clearly, by the choice of Φ, we have $\widetilde{\Delta}_\Phi \neq 0$. Specializing in (10), we see that $E = \widetilde{\Delta}_\Phi k[\rho_1,\dots,\rho_n] \subset k[\widetilde{\Psi}_1,\dots,\widetilde{\Psi}_e] \subset E$; hence $E = k[\widetilde{\Psi}_1,\dots,\widetilde{\Psi}_e]$. □

Remark 8. Theorem 7 strongly improves the result given by Dickson (see [7, pp. 190–193]).

The next theorem is a crucial tool for relating generic and specialized resolvents. Let $\Gamma = \mathrm{Gal}(E/k)$. By means of the ordering $(\rho_1,\dots,\rho_n)$ of the roots of f, the group Γ can be identified with a subgroup of $\mathfrak{S}_n$. We will do so.

Theorem 9. *Let Θ be a primitive invariant of a subgroup H of $\mathfrak{S}_n$. Put $\theta = \widetilde{\Theta}$. Assume θ is a simple root of the specialized resolvent $\mathscr{L}_{\Theta,f}$. Then* $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap H$.

Proof. For every $\sigma \in \Gamma$ and $\varphi \in \mathscr{A}$, we have

$$\widetilde{\sigma \bigstar \varphi} = \sigma(\widetilde{\varphi}) \tag{11}$$

(keep in mind that on the left-hand side of (11), σ acts as an element of $\mathrm{Gal}(\mathscr{F}/\mathscr{K})$, while on the right-hand side, it acts as an element of $\mathrm{Gal}(E/k)$). Thus, for all $\sigma \in \Gamma \cap H$ we have $\widetilde{\sigma \bigstar \Theta} = \widetilde{\Theta} = \theta = \sigma(\widetilde{\Theta}) = \sigma(\theta)$, whence $\sigma \in \mathrm{Gal}(E/k(\theta))$. This gives $\Gamma \cap H \subset \mathrm{Gal}(E/k(\theta))$.

Now, take any $\sigma \in \Gamma \backslash H$. Putting $\Theta' = \sigma \bigstar \Theta$, clearly $\Theta' \neq \Theta$. The (Θ, f)- resolvent is: $\mathscr{L}_{\Theta,f} = \prod_{\Psi \in \omega}(X - \widetilde{\Psi})$, where ω stands for the $\mathfrak{S}_n$-orbit of Θ in $\mathscr{A}$. But θ being a *simple* root of $\mathscr{L}_{\Theta,f}$, necessarily $\widetilde{\Theta}' \neq \theta$. Consequently, $\widetilde{\Theta}' = \widetilde{\sigma \bigstar \Theta} = \sigma(\widetilde{\Theta}) = \sigma(\theta)$, whence $\sigma(\theta) \neq \theta$, which implies $\sigma \notin \mathrm{Gal}(E/k(\theta))$. This gives the expected opposite inclusion: $\mathrm{Gal}(E/k(\theta)) \subset \Gamma \cap H$, ending the proof. □

3. The chasing' resolvents method

3.1. The partition matrix

The basic idea of the present paper consists of reversing the usual approach to compute Galois groups through resolvents. Rather than starting with resolvents, chosen almost randomly within the constraints of effective calculations, we construct a priori global abstract group tables. Partitions issued from the factorization of resolvents of f over the base field correspond to a row of one of our groupistic tables. These tables can be computed by means of various packages. Our calculations were performed on GAP (see [10]); another valuable system, is MAGMA (formerly CAYLEY). From the tables, we infer resolvents needed to search particular Galois groups, and not conversely.

Let n be a non-null natural integer. We will call *partition* of n any n-tuple $(\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$ verifying $\sum_{i=1}^{n} i\alpha_i = n$. (This definition recovers the usual combinatorial notion of partition.) The set $\{i \in [\![1,n]\!] \mid \alpha_i \geq 1\}$ will be called the *support* of the partition. For each $i \in [\![1,n]\!]$, the integer α_i is by definition the *multiplicity* of i in the partition. The cardinality r of the support is the *number of components* of the partition. A partition ϖ of n is characterized by two objects: the strictly increasing sequence $(d_1,\dots,d_r)$ of its support elements, and the function $[\![1,r]\!] \to \mathbb{N}^*$, $j \mapsto \nu_j = \alpha_{d_j}$. We will designate the partition as follows: $\varpi = [(\nu_1,d_1),\dots,(\nu_r,d_r)]$. In this notation, it is understood that all $\nu_i \geq 1$, $r \geq 1$, and $1 \leq d_1 < \cdots < d_r \leq n$.

In the present section, we fix once for all a finite group G, of cardinality N. Let U and V be subgroups of G. Put $e = [G : U]$, and let $\{C_1, \dots, C_e\}$ be the left coset set G/U, enumerated so that $C_1 = U$. Denote by $\mathscr{U}$ and $\mathscr{V}$, respectively, the conjugacy classes of subgroups of G containing U and V. Now consider the left action of V on G/U by left translations. Denoting α_i the number of V-orbits having cardinality i $(1 \le i \le e)$, clearly we obtain a partition $(\alpha_1, \dots, \alpha_e)$ of e, which will be designated by $\mathscr{P}(V, U)$. Then:

Proposition 10. *The above partition $\mathscr{P}(V, U) = (\alpha_1, \dots, \alpha_e)$ depends only on the conjugacy classes $\mathscr{U}$ and $\mathscr{V}$.*

Proof. We first show that the choice of U in $\mathscr{U}$ is irrelevant. Indeed, let $\sigma \in G$, and put $U' = \sigma U \sigma^{-1}$. Then we have a natural bijection $f : G/U \to G/U'$, given by $C \mapsto C\sigma^{-1}$, which is easily verified to be an isomorphism of G-sets. Thus $\mathscr{P}(V, U') = \mathscr{P}(V, U)$.

Now, we can prove the independence of $\mathscr{P}(V, U)$ on the choice of V in $\mathscr{V}$. Take $\sigma \in G$; put $V' = \sigma V \sigma^{-1}$ and $U' = \sigma U \sigma^{-1}$. The inner automorphism $I_\sigma : x \mapsto \sigma x \sigma^{-1}$ of G satisfies $I_\sigma(\gamma C) = I_\sigma(\gamma) I_\sigma(C)$ for all $\gamma \in G$ and $C \in G/U$. Hence, I_σ induces a bijection of the V-orbit set G/U onto the V'-orbit set G/U'. Therefore, $\mathscr{P}(V', U') = \mathscr{P}(V, U)$. By applying the first part of the proof, we see that $\mathscr{P}(V', U') = \mathscr{P}(V', U)$; hence $\mathscr{P}(V, U) = \mathscr{P}(V', U)$, as desired. □

In order to define our partition matrix, we order the conjugacy classes of subgroups of G, say $(\mathscr{C}_1, \dots, \mathscr{C}_s)$ (so s denotes the number of these classes). It will be convenient to choose this ordering so that the indices $([G : H])_{H \in \mathscr{C}_i}$ are decreasing functions of i; thus, $\mathscr{C}_1 = \{\{e_G\}\}$ and $\mathscr{C}_s = \{G\}$. Due to Proposition 10, to every pair $(\mathscr{U}, \mathscr{V})$ of conjugacy classes of subgroups of G, we may associate a well-defined partition, namely, the partition equal to $\mathscr{P}(V, U)$ for all choices of U in $\mathscr{U}$ and V in $\mathscr{V}$. This well-defined partition will be denoted $\varpi(\mathscr{V}, \mathscr{U})$.

Definition 11. With the above notation, the matrix $\mathscr{P}_G = \left[\varpi(\mathscr{C}_i, \mathscr{C}_j)\right]_{\left\{\substack{1 \le i \le s \\ 1 \le j \le s}\right.}$ will be called the *partition matrix* of G (associated with the chosen ordering $(\mathscr{C}_i)$).

Now we shall describe an explicit way for computing of this matrix. Take subgroups U, V of G as above. Let $e = [G : U]$; choose a left transversal $(g_1, \dots, g_e)$ of G mod U, so that $g_1 = e_G$. For $i \in [\![1, e]\!]$, put: $C_i = g_i U$, $U_i = g_i U g_i^{-1}$ (hence, $U_1 = U$). Then $\mathrm{Stab}_V(C_i) = V \cap U_i$ for all i.

Proposition 12. *The notation being as above, the partition $\mathscr{P}(V, U)$ is $(\alpha_1, \dots, \alpha_e) = (N_1/1, \dots, N_j/j, \dots, N_e/e)$, where for all j, N_j designates the number of those $i \in [\![1, e]\!]$ such that $[V : V \cap U_i] = j$.*

Proof. To each $i \in [\![1, e]\!]$, associate the index $v(i) = [V : V \cap U_i]$. Then $v(i)$ is the cardinality of the V-orbit ω_i of C_i, because $V \cap U_i = \mathrm{Stab}_V(C_i)$. Therefore, denoting

$\mathcal{N}_j$ the inverse image of a given $j \in [\![1,e]\!]$ by the mapping v, the set $\{C_i\}_{i\in\mathcal{N}_j}$ is the union of the V-orbits of cardinality j in G/U; putting $N_j = \operatorname{card}(\mathcal{N}_j)$, we see now that the total number of these V-orbits is N_j/j, as expected. □

Remark 13. Those of the above α_j's which are $\neq 0$ are not quite arbitrary. Indeed, if $\alpha_j \neq 0$, there is at least one V-orbit of cardinality j, so in this case the number j must divide $\operatorname{card}(V) = N/[G:V]$.

In order to state our next theorem, we keep the above notation $G, \mathscr{C}_1,\dots,\mathscr{C}_s$ and the above assumptions.

Theorem 14. *The rows of the partition matrix* $\mathscr{P}_G = \left[\varpi(\mathscr{C}_i,\mathscr{C}_j)\right]_{\left\{\substack{1\le i\le s\\ 1\le j\le s}\right.}$ *are distinct. Hence, they define a bijection of* $[\![1,s]\!]$ *onto the set* $\{\mathscr{C}_1,\dots,\mathscr{C}_s\}$.

Proof. For each $i \in [\![1,s]\!]$, choose a subgroup $H_i \in \mathscr{C}_i$, and denote $e_i = [G:H_i]$. Fix two integers i and j with $1 \le j < i \le s$. Let $(\alpha_1,\dots,\alpha_{e_j})$ be the partition $\varpi(\mathscr{C}_j,\mathscr{C}_j)$. Let $(\gamma_1,\dots,\gamma_{e_j})$ be a left transversal of G mod H_j, such that $\gamma_1 = 1_G$. Then, $[H_j : \gamma_1 H_j \gamma_1^{-1} \cap H_j] = 1$; the total number of integers r verifying $H_j = \gamma_r H_j \gamma_r^{-1}$ is obviously $[\mathfrak{N}_G(H_j) : H_j]$, where $\mathfrak{N}_G$ stands for "the normalizer subgroup of ... in G". Consequently, $\alpha_1 = [\mathfrak{N}_G(H_j) : H_j] \ge 1$. Now, let $(\beta_1,\dots,\beta_{e_j})$ be the partition $\varpi(\mathscr{C}_i,\mathscr{C}_j)$. For any $m \in [\![1,e_j]\!]$, we have $\gamma_m H_j \gamma_m^{-1} \neq H_i$, because $\mathscr{C}_i \neq \mathscr{C}_j$, and we cannot have $H_i \subset_{\neq} \gamma_m H_j \gamma_m^{-1}$, because $e_i \le e_j$. Hence $\beta_1 = 0$, which proves that $\varpi(\mathscr{C}_i,\mathscr{C}_j) \neq \varpi(\mathscr{C}_j,\mathscr{C}_j)$. Therefore, the ith row and the jth row of $\mathscr{P}_G$ are distinct. □

3.2. The main theorem

Now we arrive at the heart of our actual problem, how to relate the partition matrices and the resolvents. At this stage, we will restore the notation n, $\mathscr{A}$, $\mathscr{F},\mathscr{K}$, F, $f = X^n + \sum_{i=1}^n (-1)^i c_i X^{n-i}$, E, $(\rho_1,\dots,\rho_n)$ and the corresponding hypotheses made at the beginning of Section 2.2. We denote by Γ the Galois group $\operatorname{Gal}(E/k)$, and by $\mathfrak{C}$ its conjugacy class in $\mathfrak{S}_n$. The set $\mathbb{N}^n$ will be equipped with the direct product ordering issued from the natural order on $\mathbb{N}$. This ordering will be denoted $\preceq$. Thus, for $\boldsymbol{a} = (a_1,\dots,a_n) \in \mathbb{N}^n$ and $\boldsymbol{b} = (b_1,\dots,b_n) \in \mathbb{N}^n$, the assertion $\boldsymbol{a} \preceq \boldsymbol{b}$ means that $a_i \le b_i$ for all i. Recall that the result $\varphi(\rho_1,\dots,\rho_n)$ of the specialization $(X_1,\dots,X_n) \rightsquigarrow (\rho_1,\dots,\rho_n)$ in a polynomial $\varphi \in \mathscr{A} = k[X_1,\dots,X_n]$ is denoted by $\widetilde{\varphi}$.

Theorem 15. *Let Θ be a primitive invariant for a subgroup H of $\mathfrak{S}_n$. Let $\mathscr{C}$ be the conjugacy class of H in $\mathfrak{S}_n$. Put $e = [\mathfrak{S}_n : H]$. For all $j \in [\![1,e]\!]$, denote by α_j the number of the simple irreducible factors over k of $\mathscr{L}_{\Theta,f}$ having degree j. Then*:

(a) *If all these simple irreducible factors are separable, then*

$$(\alpha_1,\dots,\alpha_e) \preceq \varpi(\mathfrak{C},\mathscr{C}). \tag{12}$$

(b) *If $\mathscr{L}_{\Theta,f}$ is separable, then*

$$(\alpha_1,\dots,\alpha_e)=\varpi(\mathfrak{C},\mathscr{C}). \tag{13}$$

Proof. Take a left transversal $(\gamma_1,\dots,\gamma_e)$ of $\mathfrak{S}_n$ mod H so that $\gamma_1=\mathrm{Id}$. For $m\in[\![1,e]\!]$, put $H_m=\gamma_m H\gamma_m^{-1}$; $\Theta_m=\gamma_m\star\Theta$; $\theta_m=\widetilde{\Theta}_m$ (so, $H_1=H$; $\Theta_1=\Theta$, and $H_m=\mathrm{Stab}_{\mathfrak{S}_n}(\Theta_m)$ for all m). Then

$$\mathscr{L}_\Theta=\prod_{m=1}^{e}(X-\Theta_m),\qquad \mathscr{L}_{\Theta,f}=\prod_{m=1}^{e}(X-\theta_m).$$

For $j\in[\![1,e]\!]$, let N_j the number of those integers $m\in[\![1,e]\!]$ for which $[\Gamma:\Gamma\cap H_m]=j$. By Proposition 12, we obtain: $\varpi(\mathfrak{C},\mathscr{C})=(N_1/1,\dots,N_e/e)$.

(a) Fix $j\in[\![1,e]\!]$. Take an irreducible simple monic factor P over k of $\mathscr{L}_{\Theta,f}$ having degree j. By hypothesis, P is separable. Hence, there is a subset J of cardinality j in $[\![1,e]\!]$ such that $P=\prod_{m\in J}(X-\theta_m)$. For all $m\in J$, the degree j of P equals $[\Gamma:\Gamma\cap H_m]$ since θ_m is a simple root of $\mathscr{L}_{\Theta,f}$ (this comes from Theorem 9). There are exactly α_j such polynomials P. Thus, the set-union of the corresponding J's gives $j\alpha_j$ integers m fulfilling $[\Gamma:\Gamma\cap H_m]=j$. This implies $j\alpha_j\le N_j$. So, $\alpha_j\le N_j/j$ for all $j, 1\le j\le e$, as asserted.

(b) As $\mathscr{L}_{\Theta,f}$ is separable, now $\sum_{j=1}^{e} j\alpha_j=e$. This obviously forces the inequality (12) to be an equality. □

We now return to our problem of finding the Galois group $\Gamma=\mathrm{Gal}(E/k)$ of f. Here we take as group G the group $\mathfrak{S}_n$. We will fix an ordering $(\mathscr{C}_1,\dots,\mathscr{C}_s)$ for the conjugacy classes of subgroups of $\mathfrak{S}_n$, as explained just after Proposition 10, and we will use the corresponding partition matrix $\mathscr{P}_{\mathfrak{S}_n}=\left[\varpi(\mathscr{C}_i,\mathscr{C}_j)\right]_{\left\{\substack{1\le i\le s\\ 1\le j\le s}\right.}$ For each $j\in[\![1,s]\!]$, write $e_j=[\mathfrak{S}_n:H_j]$, choose a subgroup $H_j\in\mathscr{C}_j$ and a primitive invariant Θ_j of H_j. Let $\alpha_{j,\ell}$ be the number of irreducible factors over k of degree ℓ of $\mathscr{L}_{\Theta_j,f}$ $(1\le\ell\le e_j)$. The following result is immediate from (13).

Theorem 16. *Assume that all the above invariants Θ_j are f-separable. The conjugacy class of Γ in $\mathfrak{S}_n$ is $\mathscr{C}_r$, where r is such that the rth row of the partition matrix $\mathscr{P}_{\mathfrak{S}_n}$ coincides with $(\mathfrak{P}_1,\dots,\mathfrak{P}_s)$, where $\mathfrak{P}_j=(\alpha_{j,1},\dots,\alpha_{j,e_j})$.*

Now, the chasing' resolvents method runs as follows: first of all, the partition matrix $\mathscr{P}_{\mathfrak{S}_n}$ is displayed (we have found it entirely for $n\le 7$ using the software GAP). Then, f-separable primitive invariants Θ_j are determined, and the corresponding specialized resolvents $\mathscr{L}_{\Theta_j,f}$ are computed; it remains to factorize these resolvents over the base field and to apply Theorem 16. (Note that the existence of such Θ_j's is made sure by Theorem 6 when k has characteristic zero.) When running the chasing' resolvents method, it is convenient to view the above subgroups H_j as *test groups* (keeping in mind that only their conjugacy classes are relevant). They correspond to the columns of $\mathscr{P}_{\mathfrak{S}_n}$. On the other hand, the rows of $\mathscr{P}_{\mathfrak{S}_n}$, which also correspond to the classes $\mathscr{C}_j$,

Table 1
Representative subgroups for the conjugacy classes of $\mathfrak{S}_4$

Groups	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}	H_{11}
Nature	Id_4	$\mathrm{Id}_2 \times \mathfrak{S}_2$	$\mathfrak{S}_2$	$\mathrm{Id} \times \mathfrak{A}_3$	${\mathfrak{S}_2}^2$	V_4	C_4	$\mathrm{Id} \times \mathfrak{S}_3$	$\mathscr{D}_4$	$\mathfrak{A}_4$	$\mathfrak{S}_4$
Size	1	2	2	3	4	4	4	6	8	12	24
Invariant	$X_1X_2^2X_3^3$	$X_1X_2X_3^2$	Θ_3	δ_3	X_1X_2	Θ_6	Θ_7	X_1	Θ_9	δ_4	1

must be viewed as the *candidate subgroup classes*, because one and only one of them comes from Γ.

The importance method should not fail to strike the reader, owing to its applicability to polynomials f assumed solely to be *separable*, not necessarily irreducible over the base field k.

3.3. Improvements to the chasing' resolvents method

Of course, if all the Θ_j's and all the $\mathscr{L}_{\Theta_j,f}$'s had to be computed, this would be an almost insuperable task. Fortunately, it appears that only very few of them are needed for explicit calculations. For example, if it is known that f is irreducible over k, then only the columns of $\mathscr{P}_{\mathfrak{S}_n}$ relative to *transitive* subgroup classes of $\mathfrak{S}_n$ are required. (By a *transitive* class, we mean a class of transitive subgroups of $\mathfrak{S}_n$.) Moreover, far from all test groups are needed, as shown by direct examination of the actual partition matrices at our disposal. The heavy hypotheses of separability can be enlarged too. Finally, in many cases, the whole resolvents are not needed: some suitable factors of them may suffice.

Example 17 (*Degree* 4). We shall display the chasing' resolvents method for $n = 4$, which will suffice for a good understanding (the complete partition matrices are available for all $n \leq 7$; partial partition matrices relative to *transitive* candidates are available up to degree 11; we cannot give any of them here, for the sake of their excessive lengths). For our present purpose, we assume the characteristic of k is neither 2 nor 3. By using GAP, we first obtain groups H_j representative of the 11 conjugacy classes in $\mathfrak{S}_4$, ordered as explained above (see Table 1). In Table 1, $\Theta_3 = X_1X_3^2{+}X_2X_4^2$, $\Theta_7 = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2$, $\Theta_9 = X_1X_2 + X_3X_4$, $\Theta_6 = (X_1 - X_4)(X_3 - X_2)$, and $\delta_m = \prod_{1\leq i<j\leq m}(X_i - X_j)$. Finally, still by using GAP, we display the partition matrix $\mathscr{P}_{\mathfrak{S}_4}$ in Table 2; for brevity, we write $d_1^{v_1}, \ldots, d_r^{v_r}$ for the partition $[(v_1, d_1), \ldots, (v_r, d_r)]$; recall that the groups of the top line must be viewed as *test groups*, and the groups of the left column as *candidate groups*.

3.4. Sorting

Returning now to the general notation of Theorems 15 and 16, for all integers r and j in $[\![1,s]\!]$, denote by $\mathscr{U}_{j,r}$ the set of integers $m \in [\![1,s]\!]$ for which $\varpi(\mathscr{C}_m, \mathscr{C}_j) = \varpi(\mathscr{C}_r, \mathscr{C}_j)$. We will say that a subset J of $[\![1,s]\!]$ *sorts* the class $\mathscr{C}_r$ if and only if

Table 2
The partition matrix $\mathscr{P}_{\mathfrak{S}_4}$

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}	H_{11}
H_1	1^{24}	1^{12}	1^{12}	1^8	1^6	1^6	1^6	1^4	1^3	1^2	1
H_2	2^{12}	$1^2,2^5$	2^6	2^4	$1^2,2^2$	2^3	2^3	$1^2,2$	$1,2$	2	1
H_3	2^{12}	2^6	$1^4,2^4$	2^4	$1^2,2^2$	1^6	$1^2,2^2$	2^2	1^3	1^2	1
H_4	3^8	3^4	3^4	$1^2,3^2$	3^2	3^2	3^2	$1,3$	3	1^2	1
H_5	4^6	$2^2,4^2$	$2^2,4^2$	4^2	$1^2,4$	2^3	$2,4$	2^2	$1,2$	2	1
H_6	4^6	4^3	2^6	4^2	2^3	1^6	2^3	4	1^3	1^2	1
H_7	4^6	4^3	$2^2,4^2$	4^2	$2,4$	2^3	$1^2,4$	4	$1,2$	2	1
H_8	6^4	$3^2,6$	6^2	$2,6$	3^2	6	6	$1,3$	3	2	1
H_9	8^3	$4,8$	4^3	8	$2,4$	2^3	$2,4$	4	$1,2$	2	1
H_{10}	12^2	12	6^2	4^2	6	3^2	6	4	3	1^2	1
H_{11}	24	12	12	8	6	6	6	4	3	2	1

$\bigcap_{j\in J}\mathscr{U}_{j,r} = \{r\}$. This amounts to requiring that in the submatrix of $\mathscr{P}_{\mathfrak{S}_n}$ obtained by cancelling the columns whose index is not in J, the rows of index distinct from r are all different from the rth. Clearly, when Γ happens to belong to $\mathscr{C}_r$, in order to find Γ, the chasing' resolvents method will work with only the knowledge of the resolvents $\mathscr{L}_{\Theta_j,f}$ where j is in any set J sorting $\mathscr{C}_r$. As an example, look again at Table 2: it is seen that the invariant Θ_9, classically used for solving equations of degree 4, is a very bad one as far as sorting is concerned. On the contrary, the pair $(X_1X_2X_3^2, \delta_4)$ suffices for sorting any conjugacy class of subgroups of $\mathfrak{S}_4$.

4. Relative resolvents

In this section, we fix a subgroup L_0 of $\mathfrak{S}_n$ containing Γ, and we put $e_0 = [\mathfrak{S}_n : L_0]$. We denote by $\mathfrak{C}^{[L_0]}$ the conjugacy class of $\Gamma = \mathrm{Gal}(E/k)$ in L_0. It follows readily from (11) that $\widetilde{\varphi} \in k$ for all $\varphi \in \mathscr{A}_{L_0}$. Now, let H be a subgroup of L_0. Then the field $\mathrm{Inv}(H)$ is a separable extension of $\mathrm{Inv}(L_0)$, having degree $e = [L_0 : H]$. When k is infinite, this extension field admits primitive homogeneous elements belonging to $\mathscr{A}_H = \mathscr{A} \cap \mathrm{Inv}(H)$. For instance, take any homogeneous primitive invariant of H.

Definition 18. The notation and hypotheses being as above (no hypothesis being made on k), we will call relative primitive (generic) invariant of H with respect to L_0 any primitive element of the extension field $\mathrm{Inv}(H)/\mathrm{Inv}(L_0)$ belonging to $\mathscr{A}_H$. The minimal polynomial over $\mathrm{Inv}(L_0)$ of such an element Θ will be called relative generic resolvent associated with (Θ, H, L_0), and denoted by $\mathscr{L}_\Theta^{[L_0]}$.

Of course, we recover the previous notion of resolvent when taking $L_0 = \mathfrak{S}_n$. The latter will be called *absolute* resolvents. Let Θ be a relative primitive invariant as in the above definition. The L_0-orbit ω of Θ has $e = [L_0 : H]$ elements. Let $\omega = \{\Theta_1, \dots, \Theta_e\}$, with $\Theta_1 = \Theta$. Then

$$\mathscr{L}_{\Theta}^{[L_0]}(X) = \prod_{i=1}^{e}(X - \Theta_i). \tag{14}$$

Clearly, $\mathscr{L}_{\Theta}^{[L_0]}(X) \in \mathscr{A}_{L_0}[X]$. Specializing (through the morphism $\varphi \mapsto \widetilde{\varphi}$), we get an element of $k[X]$, which we will denote $\mathscr{L}_{\Theta,f}^{[L_0]}$, given by

$$\mathscr{L}_{\Theta,f}^{[L_0]} = \prod_{i=1}^{e}(X - \widetilde{\Theta}_i). \tag{15}$$

Hence, $\mathscr{L}_{\Theta,f}^{[L_0]}(X)$ divides the absolute resolvent $\mathscr{L}_{\Theta,f}(X)$ in $k[X]$. Putting $H' = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$, one has $H' \cap L_0 = H$, $\deg(\mathscr{L}_{\Theta,f}(X)) = [\mathfrak{S}_n : H']$, and

$$e \cdot [\mathfrak{S}_n : L_0] = [H' : H] \cdot [\mathfrak{S}_n : H']. \tag{16}$$

Definition 19. The polynomial $\mathscr{L}_{\Theta,f}^{[L_0]}(X) \in k[X]$ defined in (15) will be called relative resolvent of f associated to (Θ, H, L_0) (see [14]). The primitive invariant Θ will be said *f-separable* (or, more precisely, *(L_0, f)-separable*) if and only if $\mathscr{L}_{\Theta,f}^{[L_0]}(X)$ is separable.

Remark 20. Even in the case where $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$, the relative resolvent $\mathscr{L}_{\Theta,f}^{[L_0]}(X)$ may be separable without the absolute resolvent $\mathscr{L}_{\Theta,f}$ being so. Hence, dealing with suitable relative resolvents may be a way of throwing out multiple factors in absolute resolvents.

In view of an extension of the chasing' resolvents method to relative resolvents, we need a sharper version of Theorem 9. The notation and hypotheses are those in (14) and (15).

Theorem 21. *Let $\theta = \widetilde{\Theta}$. Denote by v the multiplicity of θ as a root of $\mathscr{L}_{\Theta,f}^{[L_0]}(X)$. Let J be the set $\{j \in [\![1,e]\!] \mid \widetilde{\Theta}_j = \theta\}$; let $M = \mathrm{Stab}_{L_0}(\{\Theta_j\}_{j \in J})$. Then*:

(a) $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap M$ *and*

$$\Gamma \cap H \subset \Gamma \cap M; \quad [\Gamma : \Gamma \cap H] \leq v \cdot [k(\theta) : k]; \quad [k(\theta) : k] = [\Gamma : \Gamma \cap M].$$

(b) *In particular, if $v = 1$, one has* $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap H$ *and* $[k(\theta) : k] = [\Gamma : \Gamma \cap H]$. *Consequently, $\theta \in k$ if and only if $\Gamma \subset H$.*

Proof. Assertion (b) follows immediately from assertion (a) by taking $v = 1$. So we prove (a).

Let $g \in \Gamma$. Fixing any $j \in J$, the condition $g(\theta) = \theta$ means $g(\widetilde{\Theta}_j) = \widetilde{\Theta}_j$, i.e. $\widetilde{g \bigstar \Theta_j} = \widetilde{\Theta}_j$ (see (11)). But $\Gamma \subset L_0$, which implies $g \bigstar \Theta_j \in \{\Theta_1, \ldots, \Theta_e\}$, so the condition $g(\theta) = \theta$ is equivalent to

$$g \bigstar \Theta_j \in \{\Theta_\ell\}_{\ell \in J}. \tag{17}$$

As this works for every $j \in J$, our condition on g amounts to $g \in M$. Moreover, if relation (17) is true for a particular $j \in J$, it implies that $g \in M$. Taking $j = 1$, this gives that $(g(\Theta) = \Theta)$ implies $g \in M$, whence $\Gamma \cap H \subset \Gamma \cap M$. Hence, it is proved that $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap M$ and $\Gamma \cap H \subset \Gamma \cap M$.

It remains to establish the inequality involving v. Note that $v = \mathrm{card}(J)$. Put $\mathscr{T} = \{\Theta_\ell\}_{\ell \in J}$. From the above, $\mathrm{Stab}_{\Gamma\cap M}(\Theta) = \Gamma \cap H$, and $\mathrm{Orb}_M(\Theta) = \mathscr{T}$. Hence, $[\Gamma \cap M : \Gamma \cap H] = \mathrm{card}(\mathrm{Orb}_{\Gamma\cap M}(\Theta)) \leq \mathrm{card}(\mathrm{Orb}_M(\Theta)) = v$. On the other hand, $[\Gamma : \Gamma \cap M] = [k(\theta) : k]$, so we finally get

$$[\Gamma : \Gamma \cap H] = [\Gamma : \Gamma \cap M] \cdot [\Gamma \cap M : \Gamma \cap H] \leq v \cdot [k(\theta) : k].$$

Now we can extend our main theorem. Keeping Θ, H and L_0 as above, for all $j \in [\![1,e]\!]$, denote by α_j the number of the k-irreducible simple factors of $\mathscr{L}^{[L_0]}_{\Theta,f}(X)$. (Hence when the latter is separable, $(\alpha_1,\ldots,\alpha_e)$ is a partition of e.) Recall that $\mathfrak{C}^{[L_0]}$ stands for the conjugacy class of Γ in L_0. The conjugacy class of H in L_0 will be denoted $\mathscr{C}^{[L_0]}$. Using Theorem 21, the following can be established without difficulty by reasoning similarly as in Theorem 15.

Theorem 22. (a) *One has* $(\alpha_1,\ldots,\alpha_e) \preceq \varpi(\mathfrak{C}^{[L_0]}, \mathscr{C}^{[L_0]})$.

(b) *Moreover, if Θ is (L_0, f)-separable, then*

$$(\alpha_1,\ldots,\alpha_e) = \varpi(\mathfrak{C}^{[L_0]}, \mathscr{C}^{[L_0]}). \tag{18}$$

For stating the relative version of our main theorem, choose an ordering $\mathscr{C}_1^{[L_0]},\ldots,\mathscr{C}_{s_0}^{[L_0]}$ for the distinct conjugacy classes of subgroups of L_0, so that their indices decrease (so, $\mathscr{C}_1^{[L_0]} = \{\{\mathrm{Id}\}\}$ and $\mathscr{C}_{s_0}^{[L_0]} = \{L_0\}$). For each integer $j \in [\![1,s_0]\!]$, let H_j be a subgroup in the class $\mathscr{C}_j^{[L_0]}$, and let Θ_j a primitive relative invariant for H_j with respect to L_0. Denote $e_j = [L_0 : H_j]$, and for $1 \leq \ell \leq e_j$, let $\alpha_{j,\ell}$ be the number of the simple k-irreducible factors of the relative resolvent $\mathscr{L}^{[L_0]}_{\Theta_j,f}$. Using (18), it is easily proved, in a way analogous to Theorem 16.

Theorem 23. *Assume that all the above Θ_j's are (L_0, f)-separable. Then the conjugacy class $\mathfrak{C}^{[L_0]}$ of Γ in L_0 is $\mathscr{C}_r^{[L_0]}$, where r is the integer such that the rth row of the partition matrix*

$$\mathscr{P}_{L_0} = \left[\varpi(\mathscr{C}_i^{[L_0]}, \mathscr{C}_j^{[L_0]})\right]_{\left\{\substack{1\leq i\leq s_0\\ 1\leq j\leq s_0}\right.}$$

coincides with $(\mathfrak{P}_1,\ldots,\mathfrak{P}_{s_0})$, *where* $\mathfrak{P}_j = (\alpha_{j,1},\ldots,\alpha_{j,e_j})$.

As a nice application of relative resolvents, we mention the completely general determination of the Galois group for a polynomial of degree 4. It must be noticed that the above resolvent $\mathscr{L}_{\Theta_9,f}$, which looked so bad, becomes a very good one when a suitable relative resolvent is joined to it. In addition, $\mathscr{L}_{\Theta_9,f}$ is always separable when f is (see [1, 6]).

5. Some theoretical properties of resolvents

5.1. Metacyclic extensions and resolvents

In this section, p designates an odd prime integer. Let M be a finite group of cardinality $p(p-1)$. Denote by C the unique p-Sylow subgroup of M. It is a characteristic subgroup, so the factor group M/C acts on C through the automorphisms $C \to C$, $x \mapsto \mu x \mu^{-1}$, where $\mu \in M$. This action will be called the *natural* action of M on C.

Definition 24. The above group M is said to be *metacyclic of degree* p if and only if it fulfills the two following conditions: the factor group M/C is cyclic, and its natural action on C is faithful.

Recall some well-known facts:

(I) A metacyclic group M of degree p is isomorphic to the group of similarities of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, i.e. the permutation group of $\mathbb{F}_p$ consisting of the bijections $x \mapsto ax + b \quad (a \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p)$.

(II) The set of the metacyclic subgroups of degree p in $\mathfrak{S}_p$ is a conjugacy class of subgroups. Its elements are the subgroups of cardinality $p(p-1)$ of $\mathfrak{S}_p$; they are maximal transitive solvable subgroups. Every transitive solvable subgroup of $\mathfrak{S}_p$ is contained in at least one metacyclic subgroup of degree p.

Definition 25. The metacyclic subgroups of degree p in $\mathfrak{S}_p$ are called the *maximal transitive metacyclic subgroups* of $\mathfrak{S}_p$.

We take $n = p$, the degree of the separable polynomial f. The two theorems below show how easy it is to compute the involved resolvents:

Theorem 26. *Assume* $p \geq 5$.

(a) *If* Γ *is* p*-cyclic, then the* k*-irreducible non-linear factors of the various separable resolvents of* f *have degree* p.

(b) *Let* $\Theta = X_1 X_2^2$. *Assume that the resolvent* $\mathscr{L}_{\Theta,f}$ *is separable and that all its* k*-irreducible factors have degree* p. *Then* Γ *is* p*-cyclic.*

Note that whenever the condition of (b) is fulfilled, then $\mathscr{L}_{\Theta,f}$ is the product of $p-1$ k-irreducible factors of degree p.

Theorem 27. *Assume* $p \geq 5$. *Let* $\Theta = X_1 X_2^2$ *and* $\Phi = X_1 X_2^2 X_3^3$. *Assume that* Θ *and* Φ *are* f*-separable. The Galois group* Γ *is metacyclic of degree* p *if and only if* $\mathscr{L}_{\Theta,f}$ *is irreducible, and* $\mathscr{L}_{\Phi,f}$ *is the product of* $p-2$ *irreducible factors of degree* $p(p-1)$.

5.2. Specialization of Galois groups

By means of resolvents, the classical Dedekind theorem about specialization of Galois groups can be highly improved. In fact, assuming that some separable irreducible resolvents remain separable irreducible under specialization, we have proved that Galois groups remain the same. In comparison, the Dedekind theorem gives only sufficient conditions under which the specialized Galois group will be a subgroup of the initial Galois group. For details, see [2].

References

[1] J.M. Arnaudiès and J. Bertin, Groupes, Algèbres et Géométrie (Ellypses, 1993).

[2] J.M. Arnaudiès and A. Valibouze, Résolvantes de Lagrange, LITP Report 93-61, 1993.

[3] E.H. Berwick, On soluble sextic equations, Proc. London Math. Soc. (2) 29 (1929) 1–28.

[4] W. Burnside, Theory of Groups of Finite Order (Dover, New York, 1955).

[5] G. Butler and J. McKay, The transitive groups of degree up to 11, Comm. Algebra 11 (1983) 863–911.

[6] A. Colin, Formal computation of Galois groups using relative resolvent polynomials, AAECC'95, Paris, Juillet, Lecture Notes in Computer Science, Vol. 948 (Springer, Berlin, 1995).

[7] L.E. Dickson, Algebraic Theories (Dover, New York, 1930).

[8] H.O. Foulkes, The resolvents of an equation of seventh degree, Quart. J. Math. Oxford Ser. (2) II (1931) 9–19.

[9] E. Galois, Oeuvres Mathématiques (SMF, Gauthier-Villars, Paris, 1897).

[10] M. Schönert et al., GAP. Groups, algorithms and programming, Lehrstuhl für Mathematik, aachen, 1993.

[11] J.L. Lagrange, Réflexions sur la résolution algébrique des équations, Oeuvres Lagrange IV (1770) 205–421.

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

[13] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. Amer. Math. Soc. 3 (1979) 475–511.

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

[15] A. Valibouze, Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problem, AAECC'95, Paris, Lecture Notes in Computer Science, Vol. 948 (Springer, Berlin, 1995).