ANNALES

DE

L'INSTITUT FOURIER

Teresa CRESPO & Zbigniew HAJTO

Differential Galois realization of double covers

Tome 52, nº 4 (2002), p. 1017-1025.

<http://aif.cedram.org/item?id=AIF_2002__52_4_1017_0>

Ann. Inst. Fourier, Grenoble
52, 4 (2002), 1017–1025

DIFFERENTIAL GALOIS REALIZATION OF DOUBLE COVERS

by T. CRESPO & Z. HAJTO

In this paper we present an effective construction of homogeneous linear differential equations of order 2 with Galois group a double cover $2G$ of a group G equal to one of the alternating groups A_4, A_5 or the symmetric group S_4 over a differential field k of characteristic 0 with algebraically closed field of constants $\mathcal{C}$. It is known that, if $K|k$ is an algebraic extension of the differential field k, then the derivation of k can be extended to K in a unique way and every k-automorphism of K is a differential one. Thus a realization of a finite group G as an algebraic Galois group over k is also a realization of G as a differential Galois group. If such a group G has a faithful irreducible representation of dimension n over $\mathcal{C}$, then G is the Galois group of a homogeneous linear differential equation of order n over k (cf. [1], [11]). The difficulty appears when one wants to find explicitly such an equation. In [2] we gave a method of construction of a homogeneous linear differential equation with Galois group $2G$ over k, starting from a polynomial with Galois group G over k, which reduces the obtention of such a differential equation to the resolution of a system of linear (algebraic) equations. In the present paper we obtain a different method which is more effective and based on the symmetric square of a differential equation. Given a polynomial $P(X) \in k[X]$ with Galois group G and splitting field K, we give an equivalent condition in terms of a quadratic form over k for the

---

T. Crespo is partially supported by the grant BFM2000-074-C02-01 of the Spanish Ministry of Education. Z. Hajto is partially supported by the grant SAB2000-0063 of the Spanish Ministry of Education.
Keywords: Picard-Vessiot extension – Symmetric square of a differential equation – Group representations.
Math. classification: 12H05 – 11F80 – 12F12.

existence of a homogeneous linear differential equation with Galois group $2G$ such that its Picard-Vessiot extension $\widetilde{K}$ is a solution to the Galois embedding problem associated to the field extension $K|k$ and the double cover $2G$ of G. When this condition is fulfiled, we determine explicitly all such differential equations. Our result has been anounced in [3].

In the sequel, k will always denote a differential field of characteristic 0 with algebraically closed field of constants $\mathcal{C}$. For the basic definitions and results of differential Galois theory we refer the reader to [4], [5] and [10].

DEFINITION 1. — *Let $L(y)=0$ be a homogeneous linear differential equation of order n over the differential field k. Let $\{y_1,\dots,y_n\}$ be a fundamental set of solutions of $L(y)=0$. We call symmetric power of order m of $L(y)=0$ the differential equation $L^{(m)}(y)=0$ whose solution space is spanned by $\{y_1^{i_1}\dots y_n^{i_n}/i_1+\dots i_n=m\}$.*

PROPOSITION 1. — *Let k be a differential field of characteristic 0 with algebraically closed field of constants $\mathcal{C}$ and*

$$L(Y)=Y''+AY'+BY=0 \tag{1}$$

an irreducible differential equation over k with Galois group a double cover $2G$ of a group G not having normal subgroups of order 2. Then the symmetric square

$$L^{(2)}(Y)=Y'''+3AY''+(2A^2+A'+4B)Y'+(4AB+2B')Y=0 \tag{2}$$

of $L(Y)=0$ has Galois group G over k.

Proof. — Let $\widetilde{K}$ be a Picard-Vessiot extension of L and K a Picard-Vessiot extension of $L^{(2)}$ contained in $\widetilde{K}$. Let (y_1,y_2) be a basis of the solution vector space of the equation $L(Y)=0$ in $\widetilde{K}$. Then $\widetilde{K}=K(y_1)$ and $[K(y_1):K]=2$. Therefore the Galois group of the extension $K|k$ is a quotient of $2G$ by a normal subgroup of order 2, which must be equal to G as G does not contain normal subgroups of order 2. The explicit expression of the coefficients of $L^{(2)}$ in terms of the coefficients of L is obtained by computing formally the derivatives of the product uv of two solutions u, v of $L(Y)=0$ (cf. [11], 3.2.2).

We shall use the following lemma on representations.

LEMMA 1. — *Let V be a k-vector space of dimension n and $\rho: G\to$ $\mathrm{GL}(V)$ an irreducible representation. Let us assume that there exists some*

$s \in G$ such that $\rho(s)$ has n different eigenvalues. We consider

$$\rho^m = \overbrace{\rho \oplus \ldots \oplus \rho}^{m} : G \to \mathrm{GL}(V^m)$$

where $V^m = \overbrace{V \oplus \ldots \oplus V}^{m}$, and we fix monomorphisms $f_j : V \to V^m$ such that $\pi_j \circ f_j : V \to V$, where π_j is the projection on the j-component, is an isomorphism of G-modules, $1 \leqslant j \leqslant m$.

Then every invariant subspace of V^m isomorphic to V as a G-module is of the form $< (\sum_j a_j f_j(v_i))_{1 \leqslant i \leqslant n} >$, for some $(a_1, \ldots, a_m) \in k^m \setminus \{(0, \ldots, 0\}$ and $(v_1, \ldots, v_n)$ a k-basis of V.

Proof. — Let $(v_1, \ldots, v_n)$ be a k-basis of V in which $\rho(s)$ diagonalizes and let $\rho(s)(v_i) = \lambda_i v_i$. Then $(f_j(v_i))_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m}$ is a basis of V^m. Let $v = \sum_{i,j} a_{ij} f_j(v_i)$. Then, if v is an eigenvector of $\rho^m(s)$ with eigenvalue λ_l, we have $\lambda_l v = \rho^m(s)(v) = \sum_{i,j} a_{ij} f_j(\rho(s)(v_i)) = \sum_{i,j} a_{ij} \lambda_i f_j(v_i)$ and so $a_{ij} = 0$ for $i \neq l$.

Let $w_l = \sum_j a_{lj} f_j(v_l), 1 \leqslant l \leqslant n$. We want to see that, if $\langle w_1, \ldots, w_n \rangle$ is an invariant subspace for ρ^m and $v_l \mapsto w_l$ defines an isomorphism of G-modules, then the coefficients a_{lj} are independent from l. For $n = 1$, there is nothing to prove. If $n > 1$, then $< v_1 >$ is not invariant and so, there exist some $t \in G$ and some $p > 1$ such that $\rho(t)(v_1) = \sum_l b_{l1} v_l$ with $b_{p1} \neq 0$. We have $\rho(t)(w_1) = \sum_l b_{l1} w_l = \sum_l b_{l1} (\sum_j a_{lj} f_j(v_l)) = \sum_{l,j} b_{l1} a_{lj} f_j(v_l)$ and, on the other hand, $\rho(t)(w_1) = \rho(t)(\sum_j a_{1j} f_j(v_1)) = \sum_j a_{1j} \sum_l b_{l1} f_j(v_l)$ and so $b_{p1} a_{pj} = b_{p1} a_{1j} \forall j \Rightarrow a_{pj} = a_{1j} \forall j$. By proceeding inductively, we prove that the coefficients a_{lj} do not depend on l.

Let now $P(X)$ be a polynomial over k with Galois group $G = A_4$, S_4 or A_5 and let K be its splitting field. We consider the Galois embedding problem $2G \to G \simeq \mathrm{Gal}(K|k)$. We recall that a solution to this embedding problem is a quadratic extension $\widetilde{K}$ of K such that the extension $\widetilde{K}|k$ is Galois and the epimorphism $\mathrm{Gal}(\widetilde{K}|k) \to \mathrm{Gal}(K|k)$, given by restriction, agrees with $2G \to G$. Therefore, if the embedding problem considered is solvable and $\widetilde{K}$ is a solution to it, then $\widetilde{K}|k$ is a differential field extension with differential Galois group $2G$ and so, is the Picard-Vessiot extension of an irreducible differential equation $L(Y) = Y'' + AY' + BY = 0$ with Galois group $2G$. The symmetric square $L^{(2)}(Y) = 0$ of $L(Y) = 0$ will be a differential equation with Picard-Vessiot extension $K|k$ and Galois group G. Moreover the symmetric square of the representation $\widetilde{\rho} : 2G \to \mathrm{GL}(2, \mathcal{C})$ associated to $L(Y) = 0$ factors through the representation $G \to \mathrm{GL}(3, \mathcal{C})$ associated to $L^{(2)}(Y) = 0$.

Let $2A_4$, $2A_5$ be the non trivial double covers of A_4 and A_5, respectively, let 2^-S_4 be the double cover of S_4 in which transpositions lift to elements of order 4, 2^+S_4 the second double cover of S_4 containing $2A_4$. In the sequel G will denote one of the groups A_4, S_4, A_5 and $2G$ one of the double covers defined above. Let us remark that each of the four groups $2G$ has a faithful irreducible representation $\widetilde{\rho}$ of dimension 2. In the sequel, ρ will stand for the irreducible representation of dimension 3 of G which is the symmetric square of $\widetilde{\rho}$. For $G = A_4$, ρ is the only irreducible representation of dimension 3 of A_4; for $G = S_4$ and $2G = 2^+S_4$, ρ is the irreducible representation of dimension 3 of S_4 contained in the permutation representation of S_4; for $G = S_4$ and $2G = 2^-S_4$, ρ is the tensor product of the representation above by the signature; for $G = A_5$, ρ is any of the two irreducible representations of dimension 3 of A_5 (which are conjugated by $\sqrt{5} \mapsto -\sqrt{5}$).

Given a polynomial $P(X)$ over k with Galois group G and a double cover $2G$ of the group G, our aim is to give a homogeneous linear differential equation of order 2 with Galois group $2G$ and such that its Picard-Vessiot extension $\widetilde{K}$ is a solution to the embedding problem considered. To this end, we shall determine the complete family of homogeneous linear differential equations with Galois group G, Picard-Vessiot extension K and associated representation ρ and among these we shall characterize the ones which are symmetric square.

We state now our main result.

THEOREM 1. — *Let k be a differential field of characteristic 0, with algebraically closed field of constants $\mathcal{C}$. Let $P(X) \in k[X]$ with Galois group $G = A_4, S_4$ or A_5, K its splitting field. Let $2G$ be a double cover of G equal to $2A_4$, 2^+S_4, 2^-S_4 or $2A_5$.*

There exist three k-vector subspaces V_1, V_2, V_3 of dimension 3 of K such that the action of G on each of them corresponds to the representation ρ and such that $V_1 + V_2 + V_3$ is a direct sum. Moreover there exists a quadratic form Q in three variables over k such that the Galois embedding problem $2G \to G \simeq \mathrm{Gal}(K|k)$ is solvable if and only if Q represents 0 over k. Let us choose a basis F_{ij}, $1 \leqslant j \leqslant 3$, in each V_i in such a way that $F_{ij} \mapsto F_{kj}$ defines an isomorphism of G-modules from V_i onto V_k. Then, for $(f,g,h) \in k^3 \setminus \{(0,0,0)\}$ such that $Q(f,g,h) = 0$, $\{fF_{1j} + gF_{2j} + hF_{3j}\}, 1 \leqslant j \leqslant 3$, is a basis of the solution space of a differential equation

$$Y''' + AY'' + BY' + CY = 0 \tag{3}$$

over k having K as Picard-Vessiot extension and such that the differential equation

$$Y'' + \frac{A}{3}Y' + \frac{1}{4}\Big(B - 2\frac{A^2}{9} - \frac{A'}{3}\Big)Y = 0 \tag{4}$$

has Galois group $2G$ over k. The coefficients A, B, C can be computed explicitly.

Proof. — Let us consider the representation of G on the k-vector space K given by the Galois action. By the normal basis theorem, this representation is the regular one and so contains ρ three times. Moreover, we can determine explicitly three k-subspaces V_1, V_2, V_3 of dimension 3 of K such that their sum $V_1 + V_2 + V_3$ is direct and such that the Galois action on $V_i, i = 1, 2, 3$, corresponds to ρ. We consider the case $G = A_4$ or S_4 and let x_1, x_2, x_3, x_4 be the roots of the polynomial P in K. When $2G = 2A_4$ or 2^+S_4, ρ is contained in the permutation representation of G on a dimension 4 vector space $< v_1, v_2, v_3, v_4 >$ and we can take $w_1 = 3v_1 - v_2 - v_3 - v_4, w_2 = 3v_2 - v_1 - v_3 - v_4, w_3 = 3v_3 - v_1 - v_2 - v_4$ as a basis of the invariant subspace W of dimension 3. The restrictions to W of the k-morphisms $< v_1, v_2, v_3, v_4 > \longrightarrow K$ given by $v_j \mapsto x_j^i$, $i = 1, 2, 3$, are monomorphisms and their images are three k-subspaces V_1, V_2, V_3 with the wanted conditions. When $2G = 2^-S_4$, ρ is contained in the representation of S_4 on a dimension 4 vector space $< v_1, v_2, v_3, v_4 >$ given by the tensor product of the permutation representation and the dimension 1 representation given by the signature and we can take $w_1 = 3v_1 - v_2 - v_3 - v_4, w_2 = 3v_2 - v_1 - v_3 - v_4, w_3 = 3v_3 - v_1 - v_2 - v_4$ as a basis of the invariant subspace W of dimension 3. The restrictions to W of the k-morphisms $< v_1, v_2, v_3, v_4 > \longrightarrow K$ given by $v_j \mapsto \sqrt{d}x_j^i$, $i = 1, 2, 3$, where d is the discriminant of the polynomial P, are monomorphisms and their images are three k-subspaces V_1, V_2, V_3 with the wanted conditions.

In the case $G = A_5$, ρ is contained in the third symmetric power of the permutation representation of G and we obtained explicitly in [1] an invariant subspace corresponding to ρ. From this explicit determination, we obtain V_1, V_2, V_3 considering, as above, the action of A_5 on the roots of the polynomial P, their squares and their cubes.

We want to determine the complete family of homogeneous linear differential equations of order 3 over k whose Picard-Vessiot extension is K and such that the corresponding representation of the group G is ρ. This is equivalent to determining the whole family of invariant subspaces V of dimension 3 of the G-module K such that the restriction of the Galois action to V corresponds to ρ. By Lemma 1, each such V is generated by $\{fF_{1j}+gF_{2j}+hF_{3j}\}_{1\leqslant j\leqslant 3}$ for F_{ij} as in the statement of the theorem and $(f,g,h)\in k^3\setminus\{(0,0,0)\}$.

We impose now that (V,ρ) is the symmetric square of the faithful representation $(\widetilde{V},\widetilde{\rho})$ of dimension 2 of $2G$. To this end, we use the explicit expression of $\widetilde{\rho}$ given in [7]. For (v_1,v_2) a basis of $\widetilde{V}$, we compute the representation ρ in the basis (v_1^2,v_1v_2,v_2^2) of the symmetric square $\widetilde{V}^{(2)}$ of $\widetilde{V}$ and consider an isomorphism φ of G-modules from $\widetilde{V}^{(2)}$ into V. We write down $\varphi(v_1^2)\varphi(v_2^2)-\varphi(v_1v_2)^2$ in the basis $\{fF_{1j}+gF_{2j}+hF_{3j}\}_{1\leqslant j\leqslant 3}$ and observe that this expression is a homogeneous polynomial of degree 2 in f,g,h whose coefficients are invariant by the action of the group G. We obtain then that (V,ρ) is the symmetric square of $(\widetilde{V},\widetilde{\rho})$ if and only if (f,g,h) satisfies an algebraic homogeneous equation $Q(f,g,h)=0$ of degree 2 with coefficients in k. The coefficients of Q are obtained explicitly in terms of the coefficients of the polynomial P. Namely, for $P(X)=X^4+s_2X^2-s_3X+s_4$ with Galois group $G=A_4$ or $G=S_4$ and $2G=2A_4$ or $2G=2^{\pm}S_4$, we obtain $Q(f,g,h)=8s_2f^2+(16s_4-4s_2^2)g^2+(8s_2^3-3s_3^2-24s_2s_4)h^2-24s_3fg+(32s_4-16s_2^2)fh+28s_2s_3gh$; for $P(X)=X^5+s_2X^3-s_3X^2+s_4X-s_5$ with Galois group $G=A_5$ and discriminant $d=D^2$ and $G=2A_5$, we obtain $Q(f,g,h)=(24s_2^3+90s_3^2-80s_2s_4)f^2+(24s_2^3s_3^2+90s_3^4-56s_2s_3^2s_4-8s_2^2s_4^2+32s_4^3-96s_2^2s_3s_5+320s_3s_4s_5)g^2+(24s_2^9+162s_2^6s_3^2+96s_2^3s_3^4-216s_2^7s_4-288s_2^4s_3^2s_4-72s_2s_3^4s_4+648s_2^5s_4^2+216s_2^2s_3^2s_4^2-728s_2^3s_4^3+48s_3^2s_4^3+240s_2s_4^4-684s_2^5s_3s_5-216s_2^2s_3^3s_5+1356s_2^3s_3s_4s_5+72s_3^3s_4s_5-1152s_2s_3s_4^2s_5+570s_2^4s_5^2+144s_2s_3^2s_5^2-900s_2^2s_4s_5^2+810s_4^2s_5^2)h^2-(24s_2^3s_3+90s_3^3-68s_2s_3s_4-60s_2^2s_5+200s_4s_5)fg-(24s_2^6+130s_2^3s_3^2-160s_2^4s_4+6s_2s_3^2s_4+304s_2^2s_4^2-160s_4^3-456s_2^2s_3s_5+30s_3s_4s_5+350s_2s_5^2+2\sqrt{5}Ds_2)fh+(24s_2^6s_3+130s_2^3s_3^3-152s_2^4s_3s_4+24s_2s_3^3s_4+292s_2^2s_3s_4^2-184s_3s_4^3-24s_2^5s_5-510s_2^2s_3^2s_5+92s_2^3s_4s_5+12s_3^2s_4s_5-20s_2s_4^2s_5+630s_2s_3s_5^2-250s_5^3+2\sqrt{5}Ds_5)gh$.

For $(f,g,h)\in k^3\setminus\{(0,0,0)\}$ such that $Q(f,g,h)=0$, we can compute explicitly a differential equation of order 3 with $\{fF_{1j}+gF_{2j}+hF_{3j}\}$ as a basis of the solution vector space. Taking into account the explicit expression of the symmetric square of a differential equation of order 2 given in Proposition 1, we obtain the equation with Galois group $2G$.

Remark 1. — For $G=S_4$ or A_4, $2G=2A_4$ or $2^{\pm}S_4$, we have $Q_E=\,<1>+Q$ where Q_E denotes the quadratic trace form of the extension $E|k$, where $E=k[X]/(P(X))$ (cf [8]). We can check that, under the hypothesis $-1,2\in k^{*2}$, the solvability condition for the Galois embedding problem $2G\to G\simeq\mathrm{Gal}(K|k)$ given in the statement of the theorem is equivalent with the one given by Serre in [8] in terms of the quadratic trace form Q_E.

Remark 2. — If the transcendence degree of k over $\mathcal{C}$ is equal to one, in particular for $k = \mathcal{C}(T)$, every quadratic form Q in three variables represents 0 over k (cf. [9] II 3.3).

Examples. — From the explicit expression of the quadratic form Q, we see that if $P(X) = X^4 - s_3X + s_4$ is a polynomial with Galois group A_4 or S_4, or $P(X) = X^5 + s_4X - s_5$ is a polynomial with Galois group A_5, then the corresponding quadratic form Q satisfies $Q(1,0,0) = 0$ and so the differential equation with solution vector space V_1 is a quadratic square. From the polynomials generating a regular extension of $\mathbb{Q}(T)$ with Galois groups A_4, S_4 and A_5 given in [6], we obtain the following differential equations:

1. The polynomial $X^4 - \frac{1}{1+3T^2}(4X-3)$ has Galois group A_4 over $\overline{\mathbb{Q}}(T)$. From it we obtain the equation

$$Y''' + \frac{18T}{1+3T^2}Y'' + \frac{115+729T^2}{12(1+3T^2)^2}Y' + \frac{27T}{4(1+3T^2)^2}Y = 0$$

with Galois group A_4, which is the symmetric square of the equation

$$Y'' + \frac{6T}{1+3T^2}Y' + \frac{43+81T^2}{48(1+3T^2)^2}Y = 0$$

with Galois group $2A_4$.

2. The polynomial $X^4 - T(4X-3)$ has Galois group S_4 over $\overline{\mathbb{Q}}(T)$. From it we obtain the equation

$$Y''' + \frac{3(-1+2T)}{2(-1+T)T}Y'' + \frac{-27+128T}{144(-1+T)T^2}Y' + \frac{3}{32(-1+T)T^3}Y = 0$$

with Galois group S_4, which is the symmetric square of the equation

$$Y'' + \frac{-1+2T}{2(-1+T)T}Y' + \frac{-27-16T}{576(-1+T)T^2}Y = 0$$

with Galois group 2^+S_4.

From the same polynomial, we obtain the equation

$$Y''' - \frac{3}{T}Y'' + \frac{999-1883T+992T^2}{144(-1+T)^2T^2}Y' + \frac{2268-6459T+6215T^2-2240T^3}{288(-1+T)^3T^3}Y = 0$$

with Galois group S_4, which is the symmetric square of the equation

$$Y'' - \frac{1}{T}Y' + \frac{567 - 1019T + 560T^2}{576(-1+T)^2T^2}Y = 0$$

with Galois group 2^-S_4.

3. The polynomial $X^5 - \frac{1}{1-5T^2}(5X-4)$ has Galois group A_5 over $\overline{\mathbb{Q}}(T)$. From it we obtain the equation

$$Y''' + \frac{3(25T^2 - (8/\sqrt{5})T + 19)}{4(-1+5T^2)^2}Y' + \frac{-75(25T^3 + (-12/\sqrt{5})T^2 + 43T - (4/5\sqrt{5}))}{20(-1+5T^2)^3}Y = 0$$

with Galois group A_5, given in [1], which is the symmetric square of the equation

$$Y'' + \frac{3(25T^2 - (8/\sqrt{5})T + 19)}{16(-1+5T^2)^2}Y = 0$$

with Galois group $2A_5$.

Different explicit examples obtained from polynomials with Galois group S_4 and A_5 whose corresponding quadratic form Q does not satisfy $Q(1,0,0) = 0$ are given in [3].

BIBLIOGRAPHY

[1] T. Crespo, Z. Hajto, Finite linear groups as differential Galois groups, Bull. Pol. Ac. Math., 49, n° 4 (2001), 363–375.

[2] T. Crespo, Z. Hajto, Primitive unimodular groups of degree 2 as differential Galois groups, J. of Algebra, 229 (2000), 678–694.

[3] T. Crespo, Z. Hajto, Recouvrements doubles comme groupes de Galois différentiels, C.R. Acad. Sci. Paris, Série I, 333 (2001), 271–274.

[4] I. Kaplansky, An introduction to differential algebra, Hermann, 1976.

[5] A.R. Magid, Lectures on differential Galois theory, A.M.S., 1997.

[6] G. Malle, B.H. Matzat, Inverse Galois Theory, Springer-Verlag, Berlin, 1999.

[7] G.A. Miller, H.F. Blichfeldt, L.E. Dickson, Theory and applications of finite groups, John Wiley and sons, Inc., 1916.

[8] J-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Comment. Math. Helvetici, 59 (1984), 651–676.

[9] J-P. Serre, Cohomologie galoisienne, cinquième édition, Springer Verlag, 1994.

[10] M.F. Singer, An outline of differential Galois theory, in Computer Algebra and Differential Equations, E. Tournier ed., Academic Press, 1989, 3–57.

[11] M.F. SINGER, F. ULMER, Galois groups of second and third order linear differential equations, Journal of Symbolic Computation, 16 (1993), 9–36.

Manuscrit reçu le 19 juillet 2001,
accepté le 4 février 2002.

Teresa CRESPO and Zbigniew HAJTO*,
Universitat de Barcelona
Departament d'Àlgebra i Geometria
Gran Via de les Corts Catalanes 585
08007 Barcelona (Spain).
crespo@cerber.mat.ub.es
rmhajto@cyf-kr.edu.pl

**Permanent address*:
Zakład Matematyki
Akademia Rolnicza
al. Mickiewicza 24/28
30-056 Kraków (Poland).