Revista de la
Unión Matemática Argentina
Vol. 35 1990.

POLYNOMIALS WITH A GIVEN GALOIS GROUP

AUGUSTO NOBILE

Respetuosamente dedicado a la memoria del Profesor Julio Rey Pastor.

Introduction

The present note is motivated by the following considerations. An open problem in the theory of singularities asks: is any germ (V,0) of complex analytic hypersurface topologically equivalent to an algebraic germ? This means: if V is defined, near $0 \in \mathbf{C}^{r+1}$, by a convergent power series $f(x_1, \ldots, x_r, x)$ (which, by Weierstrass Preparation Theorem may be assumed to be a monic polynomial in x) can we find a polynomial $p(x_1, \ldots, x_r, x)$ such that the hypersurface W: $p = 0$ is, near the origin, homeomorphic to V, via a homeomorphism which extends to one of neighborhoods of the origins? If V is smooth the solution is very simple, and if V has, at 0, an isolated singularity, the problem was solved (in the formal case and in a stronger form, namely that (V,0) and (W,0) are isomorphic germ of varieties) by P. Samuel ([S]). His technique is to show that if $f \equiv g \bmod (x_1, \ldots, x_r, x)^c$, c large enough (depending on f only), then the local rings $\mathbf{C}[[x_1, \ldots, x_r, x]] / (f)$ and $\mathbf{C}[[x_1, \ldots, x_r, x]] / (g)$ are isomorphic. Thus, a high order truncation of f will work. This becomes false if V does not have an isolated singularity at the origin (consider e.g., $x^2 - x_1^2$ and $x^2 - x_1^2 + x_2^2$, c arbitrarily large). For the generalizalition of Samuel's result to non-embedded isolated singularities, see [A1]. For a partial solution to the quoted general problem, see [N], here the problem is solved in case there is a linear projection of V on $\mathbf{C}^r$ such that the branch locus is algebraic (a condition always satisfied if r=2), as a consequence of a more general theorem on Zariski saturations of certain local rings. The techniques used in [N] are not purely algebraic.

To attack the posed problem, one is tempted to follow Samuel's approach, not simply replacing f by any algebraic series p close to f in the $(x_1, \ldots, x_r, x)$-adic topology, but by choosing one satisfying some extra requirements. Essentially, this is what is done in [A1] and [N]. In the present note we obtain, in a purely algebraic way, a little result in this direction. Recall that if (V,0) is the germ defined by

$$(1) \qquad f = x^n + a_1 x^{n-1} + \ldots + a_n, \quad a_i \in \mathbf{C}\{x_1, \ldots, x_r\},$$

then one defines its monodromy group (relative to the projection $(x_1, \ldots, x_r, x) \to (x_1, \ldots, x_r) \in \mathbf{C}^r$). One considers the natural action of $\Pi_1(U - \Delta, P)$ (where U is a suitable neighborhood of $0 \in \mathbf{C}^r$, Δ is the discriminant of the projection $\Pi : V \to U$ and $P \in U - \Delta$) on the fiber $\Pi^{-1}(P)$; when the points of this fiber are ordered in a certain way this gives us a homomorphism $\Pi_1(U - \Delta, P) \to S_n$ (the symmetric group) whose image is, by definition, the monodromy group.

It is well known that this group can be identified to the Galois group $\mathcal{G}$ (K,f) of the polynomial $f \in K[x]$, K being the fraction field of $C\{x_1,...,x_r\}$. Thus we may define, purely algebraically, $\mathcal{G}$ (K,f) to be the monodromy group of f.

Now, if (using the notation of the beginning) V and W are homeomorphic, via a homeomorphism commuting with the projections on the hyperplane $x = 0$, then certainly the monodromy groups must be isomorphic. In Section 2 we shall prove that if f (as in (1)) is given, then we may find $h = x^n + b_1 x^{n-1} + \ldots + b_n$ defining an algebraic germ of hypersurface, having the same monodromy group as f, moreover b_i can be taken arbitrarily close to a_i in the $(x_1,...,x_r)$ -adic topology, for all i. Perhaps a refinement of the methods would yield better results. This theorem is a consequence of another result (Theorem 1) that says, essentially, that the Galois group of a polynomial can be "controlled" by certain equations and inequalities involving the coefficients of the polynomial, plus some auxiliary variables; a result that might have some independent interest. The result on monodromy groups will follow easily, using Artin's Approximation Theorem ([A1], Th.1.10). Again it seems reasonable to ask whether one can get a more "economical" description of the Galois group, by using fewer auxiliary variables.

Section 1

Throughout this section, K denotes an infinite field. We shall deal with Galois groups $\mathcal{G}$ (K,f) over K of monic polynomials $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in K[x]$ without multiple roots, where n is relatively prime to the characteristic exponent of K (i.e., max (1, ch(K))). As usual, this means the Galois group of K' over K, where K' is the splitting field of f; this is $K' = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f . We assume they are in L, an algebraically closed field containing K, fixed once and for all. If the roots are ordered, then $\mathcal{G}$ (K,f) gets identified to a subgroup G of S_n , the permutations of $\{1, \ldots, n\}$; if the order of the roots is changed, we obtain a subgroup $G' \subset S_n$, conjugate to G. We are interested in the set C of conjugacy classes of subgroups of S_n, the symbol [G] will denote the class of the group G.

Monic polynomials of degree n over K are parametrized by K^n, via $a = (a_1, \ldots, a_n) \to f_a = x^n + \sum_{i=1}^{n} a_i x^{n-i}$. Polynomials without multiple roots will be called separable (some books use a different terminology). We want to show the following result.

Theorem 1. *Fix a conjugacy class $\gamma \in C$, let $S_\gamma = \{a \in K^n : f_a$ is separable and $\mathcal{G}$ (K,f_a) $= \gamma$. Then, S_γ is the image of a Zariski locally closed set $\mathcal{W}_\gamma \subset K^{2n+2}$, via the projection on the first n coordinates. Moreover, $\mathcal{W}_\gamma$ is the difference of two hypersurfaces, defined by equations with coefficients in* **Z**.

In the course of the proof we shall see more precisely which equations they are. This will be important for applications in Section 2.

Theorem 1 will be a consequence of some known results on actual constructions of Galois groups, which appear in Postnikov's book [P1]. We shall review this work (to my knowledge, this has not been translated from the Russian, the partial translations [P2] and [P3] of the book do not contain that part).

Essentially, in [P_1] the following is done. Fix a subgroup G of S_n , $G = \{e = u_1,...,u_s\}$. Take elements $v_1, \ldots, v_m$ is S_n , which represent all the right cosets of G. We shall introduce a polynomial P in variables $A_1, \ldots, A_n$, $C_1, \ldots, C_n$, T, Z, called the determining polynomial of G (often we shall use vector notation for the variables: $X = (X_1,...,X_n)$, etc.). Note first that there is a natural action on the right of S_n on polynomials involving $X_1,...,X_n$: if $\varphi = \varphi(X_1, \ldots, X_n)$ then for v in S_n, $\varphi_v = \varphi(X_{v(1)}, \ldots, X_{v(n)})$ (we must write $(vw)(i) = w(v(i))$) . We shall also write $\varphi_v = \varphi(X_v 0)$, or $\psi(Cv)$ (if the action is on the C 's) etc . The index notation will be reserved for the action on the X's only.

To construct P, consider the auxiliary variables $X = (X_1,...,X_n)$ and the polynomial

$$h(X,C) = C_1X_1 + \ldots + C_nX_n \ .$$

Let

$$\varphi(X, C, T) = \prod_{u \in \Gamma} (T - h_u(X, C)) \tag{1.1}$$

and also

$$\tilde{P} = \prod_{j=1}^{m} (Z - \varphi_{v_i}(X, C, T)) \ . \tag{1.2}$$

This polynomial, evidently with integral coefficients, is invariant under the action of S_n on X, hence it can be written as

$$P = P(A_1, \ldots, A_n, C_1, \ldots, C_n, T, Z) \ , \tag{1.3}$$

where $(-1)^j A_j$ = j-th elementary symmetric function in $X_1,\ldots,X_n$ (these are again indeterminates). Again P has integral coefficients. This is called the determining polynomial of G (indeed, its roots (in $\mathbf{Z}[X,C,T]$) are $\varphi_{v_i}(X,C,T)$, i=1,...,m and the stabilizer of φ_{v_i} under S_n is $v_i^{-1} G v_i$, so it determines G up to conjugacy). This polynomial was constructed by fixing G and $v_1, \ldots, v_m$. With G fixed, the choice of the representatives v_i of the cosets of G does not matter, while if our G is replaced by its conjugate $G' = w^{-1} G w$, $w \in S_n$, the new P' that results satisfies:

$$P'(A,C,T,Z) = P(A, C_w, T, Z) \ , \tag{1.4}$$

as a straightforward calculation shows. Also we have:

$$\varphi'(X, C, T) = \varphi_w(X, C_w, T) \ , \tag{1.5}$$

where φ' is analogous to (1.1), using G' rather than G.

The following facts are proved in [P1]. Take $a = (a_1, \ldots, a_n) \in K^n$, such that the polynomial f_a has distinct roots $(\alpha_1, \ldots, \alpha_n)$ in L, elements $c_1, \ldots, c_n$ in K, all distinct, and $t \in K$ such that

$$\varphi_{v_i}(X, c, t) \neq \varphi_{v_j}(X, c, t) \ , \quad \text{if } i \neq j \ . \tag{1.6}$$

Let

$$g(Z) = \tilde{P}(a, c, t, Z) = P(a, c, t, Z) \tag{1.7}$$

The roots of g will be $\varphi_{v_i}(\alpha, c, t)$, $i = 1, \ldots, m$. Then,

(a) If $\mathcal{G}(K, f_a)$ is a subgroup of G, then the root $\varphi(\alpha, c, t)$ of g is in K (this root corresponds to the v_i representing the coset G, say $v_1 = e$).

(b) If g(Z) does not have multiple roots and one of its roots (say, $\varphi_{v_i}(\alpha, c, t)$) is in K, then $\mathcal{G}(K,f) \subset v_i^{-1} G v_i$.

(c) Let $G_0, \ldots, G_q$ be fixed subgroups of S_n, $P_0, \ldots, P_q$ their determining polynomials, let $a \in K^n$ (as above) be given, also fix an infinite subset $B \subset K$. Then, we may choose elements $c_1, \ldots, c_n$, t in B, such that $P_i(a, c, t, Z)$ is separable for all i (in [P1] only the case q = 0 is treated, but the method of proof yields this more general result).

Now we may prove Theorem 1. Fix a group G such that $[G] = \gamma$; let $G_1, \ldots, G_q$ be all its maximal proper subgroups. Construct the determining polynomials (cf. (1.3)) of $G, G_1, \ldots, G_q$,

say $P_0 = P, P_1, \ldots, P_q$ respectively. Let $E, D_0, \ldots, D_q$ be the discriminants of $x^n + A_1 x^{n-1} + \ldots + A_n$, $P_0, \ldots, P_q$ respectively (the latter regarded as polynomials in Z, thus $E \in Z[A]$, $D_i \in Z[A,C,T]$, for all i). Let

$$(1.8) \qquad Q = \prod_{i<j} (C_i - C_j) \cdot \prod_{1 \le i \le j} P_i \cdot \prod_{i=0}^{q} D_i(A, C, T) \cdot E(A) .$$

Then, I claim that the locally closed set $\mathcal{W}_\gamma$ in K^{2n+2} defined by

$$(i)\ P = 0 , \qquad (ii)\ Q \neq 0 ,$$

can be taken as the set $\mathcal{W}_\gamma$ of Theorem 1. Let us check that if $M = (a,c,t,z) \in \mathcal{W}_\gamma$, then f_a has $[\mathcal{G}(K, f)] = \gamma$. First of all, (ii) implies $E \neq 0$ at M, hence f_a is separable, let $\alpha_1, \ldots, \alpha_n$ be its roots. Using this ordering, $\mathcal{G} = \mathcal{G}(K, f_a) \subset S_n$. Also (ii) implies $D_0 \neq 0$ at M, hence $P(a, c, t, Z)$ is separable. We are assuming that z is a root of this, hence $z = \varphi_{v_i}(\alpha, c, t)$ for some i. Write, to simplify, $v_i = v$. Then I claim: $\mathcal{G} = v^{-1} G v$. Note first that $G'_j = v^{-1} G_j v$, $j = 1, \ldots, q$, are all the maximal subgroups of G'. Use $G', G'_1, \ldots, G'_q$ to construc determining polynomials $P' = P'_0, \ldots, P'_q$ respectively. We have, by (1.4),

$$(1.9) \qquad P'_j(A, C, T, Z) = P_j(A, C_v, T, Z), \text{ all } j ;$$

also $z = \varphi_v(\alpha,c,t) = \varphi'(\alpha, c_{v-1}, t)$ (cf.(1.5)).It follows that $z = \varphi'(\alpha, c_{v-1}, t)$ is a root of $P'(a, c_{v-1}, t, Z)$. By (b) above (it is clear that $D_0 \neq 0$ at (a,c,t) implies that this polynomial is separable), $\mathcal{G} \subset G'$. Now I claim that $\mathcal{G} \not\subset G'_j$ $j = 1, \ldots, \theta$, which proves that $G = G'$. In fact, were $\mathcal{G} \subset G'_j$, then by (a) $\varphi'(\alpha, c_{v-1}, t)$ should be a root of $P'_j(a, c_{v-1}, t, Z)$, hence by (1.9) $P_j(a, c, t, z) = 0$, contradicting the fact that $Q(a, c, t, z) = 0$.

To finish, we should see that the projection maps $\mathcal{W}_\gamma$ onto $\mathcal{S}_\gamma$. So, let $a \in K^n$ be such that f_a is separable and $[\mathcal{G}(K, f_a)] = \gamma$. By (c) above we get (c,t) such that $P_j(a, c, t, Z)$ is separable, $j = 0, \ldots, q$. Order the roots $\alpha_1, \ldots, \alpha_n$ of f_a, let $G' = \mathcal{G}(K, f_a) \subset S_n$. This G'is conjugate to G, then $G' = v^{-1} G v$, $v = v_i$, for a suitable i. Working as in the first part, it is easy to see that $z = \varphi'(\alpha, c_{v-1}, t)$ is such that (a,c,t,z) satisfies (i) and (ii), i.e., it is a point of $\mathcal{W}_\gamma$. This proves that the projection $\mathcal{W}_\gamma \to \mathcal{S}_\gamma$ is surjective, concluding the proof of Theorem 1.

Section 2

Here we deal primarily with polynomials with coefficients in certain rings. Precisely, let R be the henselization of an algebra of finite type over a field or an excellent discrete valuation ring at a prime ideal, moreover we assume that R is an infinite, integrally closed integral domain.

Let $\hat{R}$ be the completion of R at a proper ideal M of R, and F(resp. K) the field of fractions of R (resp. $\hat{R}$). We fix an algebraic closure L of K. Given polynomials $f \in K[x]$ (resp. $h \in F[x]$) of degree n without multiple roots, we may regard the Galois group $\mathcal{G}(K,f)$ (resp. $\mathcal{G}(F, h)$) as a subgroup of S_n, by considering its roots, as in Section 1. This subgroup is determined up to inner automorphism (depending on the ordering of the roots). We keep the notation of Section 1, and we have:

Theorem 2. *Given a separable polynomial*

$$(2.1) \qquad f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \hat{R}[x] ,$$

(whith n relatively prime to the characteristic exponent of K) and a positive integer c, then there is a separable polynomial

(2.2) $$h(x) = x^n + b_1 x^{n-1} + \ldots + b_n \in R[x],$$

such that $b_i \equiv a_i$ *(mod* $\mathcal{M}^c$*) (where* $\mathcal{M}$ *is the maximal ideal of* R*) with* $[\mathcal{G}(K, f)] = [\mathcal{G}(K, h)] = [\mathcal{G}(F, h)]$.

Before proving the theorem, note that we have the following immediate

Corollary 1. *Fix a conjugacy class* γ *of subgroups of* S_n, let $\mathcal{P}_\gamma = \{(a_1, \ldots, a_n) = a \in \hat{R}^n : f_a$ *is separable and* $[\mathcal{G}(K, f_a)] = \gamma\}$. *Consider* $\hat{R}$ *with the* $\mathcal{M}$*-adic topology and* $\hat{R}^n$ *with the product topology.*

Then, $\mathcal{P}_\gamma \cap R^n$ *is dense in* $\mathcal{P}_\gamma$.

The following special case has geometric interest. Assume R is the henselization of the polynomial ring $k[x_1, \ldots, x_r]$ at $(x_1, \ldots, x_r)$ (k a field). Then, $R = k[[x_1, \ldots, x_r]]$ (formal power series) and R is the set of power series, algebraic over $k[x_1, \ldots, x_r]$. Given f as in Theorem 2, the group $\mathcal{G}(K, f)$ may be called the monodromy group of f. In the Introduction it is explained how this corresponds to the classical concept. It is also well-known that, under the present assumptions, h (of Theorem 2) will be algebraic, i.e., after a change of variables in $k[[x_1, \ldots, x_r, x]]$, the ideal (h) will be generated by a polynomial.

Thus, we have:

Corollary 2. *Given* $f \in k[[x_1, \ldots, x_r]][x]$ *as in* (2.1), *and an integer* $c > 0$, *then we can find an algebraic* h *as in* (2.2), *with* $a_i \equiv b_i$ *(mod* $(x_1, \ldots, x_r)^c$*)*, $i = 1, \ldots, n$, *preserving the monodromy group of f.*

In more geometric terms, we may say that it is possible to arbitrarily approximate ($\mathcal{M}$-adically) any algebroid singularity by an algebraic one, preserving its monodromy group (here we are dealing, of course, with singularities of hypersurfaces).

Now we prove Theorem 2. By ordering the roots $\alpha_1, \ldots, \alpha_n$ of our polynomial f, the Galois group $\mathcal{G}(K, f)$ gets identified to a subgroup G of S_n. Let $G_1, \ldots, G_q$ be the maximal proper subroups of G. Consider the conditions (i) and (ii) in the proof of Theorem 1, where the polynomials P and Q are constructed using $G, G_1, \ldots, G_q$. Using (c) of Section 1, applied with B = R, we get elements $c_1, \ldots, c_n, t$ in R, such that each P_i (the determining polynomial of G_i), $i = 0, \ldots, q$, with $P_0 = P$, is separable. Hence, $D_j(a, c, t) = 0$ (all j), $E(a) = 0$ (f is separable) and $c_i - c_j = 0$, $i < j$. Then, by (b) of Section 1, there is a root $z \in K$ of $P(a, c, t, Z)$. But since R is integrally closed, $z \in R$. This z cannot be a root of $P_i(a, c, t, Z)$, $i > 0$: by (b), $G(K, f)$ would be contained in a conjugate of G_i, and for cardinality reasons it could not be isomorphic to G. Thus, $(a, c, t, z) \in W_\gamma$, $\gamma = [G]$ (the set of Theorem 1). Using Artin's Approximation Theorem ([A_1], Th. 1.10) we may find, for any positive integer d, a solution (b,c',t',z') of $P = 0$, with entries in R, congruent to (a, c, t, z) modulo d. But the inequality $Q(a, c, t, z) \neq 0$ means $Q(a, c, t, z) \equiv 0 \bmod \mathcal{M}^\delta$, δ large enough. If we take $d = \max(c, \delta)$, then the point $(b,c',t',z') \in \mathcal{W}_\gamma$ and $h = f_b$ has Galois group (over K) isomorphic to G.

Now, if we use F as our base field, the conditions of Theorem 1 relative to γ are again $P = 0$, $Q \neq 0$ (the same polynomials as before). Since the entries in (b,c',t',z') are in $R \subset F$, again Theorem 1 tells us that $[\mathcal{G}(F, h)] = \gamma$.

This completes the proof of Theorem 2.

Remark. Since $C\{x_1, \ldots, x_r\}$ is henselian, it is clear that the result announced in the Introduction is a special case of Corollary 2.

References

[A1] ARTIN, M., *Algebraic approximation of structures over complete local rings*, Publ. Mat. I.M.E.S., 36 (1969), 23-58.

[A2] ARTIN, M. ,*On the solutions of analytic equations*, Inv. Math., 5 (1968), 277-291.

[N] NOBILE , A. ,*On saturations of embedded analytic rings*, Illinois J. Math., 24 (1980), 483-525.

[P1] POSTNIKOV, M.M., *Galois Theory* (in Russian), Fitmatgiz, Moscow (1963).

[P2] POSTNIKOV, M.M., *Foundations of Galois Theory*, Pergamon Press (Mac Millan), New York (1962).

[P3] POSTNIKOV, M.M., *Foundations of Galois Theory*, Gordon and Breach (Hindustan Publ. Co.) New York (1961).

[S] SAMUEL, P. ,*Algébricité de certains points singuliers algébroides*, J. Math. Pures Appl., 35 (1960) 1-6.

Louisiana State University
Department of Mathematics
Baton Rouge, Louisiana, 70803, U.S.A.

Recibido por U.M.A. el 16 de mayo de 1989.