LE MATEMATICHE
Vol. LV (2000) – Fasc. II, pp. 229–237

ATTEMPTS TO USE THE POWER OF MODERN GROUP THEORY OF FINITE SIMPLE GROUPS FOR CALCULATING GALOIS GROUPS

SHREERAM S. ABHYANKAR

Dedicated to Silvio Greco in occasion of his 60-th birthday.

This is the text of my lectures in Catania (Sicily) in April 2001, and at a Group Theory Conference in Oberwohlfach (Germany) in April 1997. The Catania visit was in honor of the 60-th birthday of my good friend Sylvio Greco.

The muse of poetry is responsible for the above poetic rendition of the original title of my talk which was more like "Recognition Theorems and Galois Theory" or "Nice Equations for Nice Groups." At any rate, various Recognition Theorems of Group Theory provide powerful tools for computing Galois groups. Examples of such Recognition Theorems are:

(1) CT = Classification Theorem of Finite Simple Groups,
(2) CDT = Classification of Doubly Transitive Permutation Groups (using CT),
(3) CR3 = Classification of Rank 3 Permutation Groups (again using CT),
(4) Jordan-Margraff Theorems on Limits of Transitivity,
(5) Burnside's Theorem (which is a special case of the O'Nan Scott Theorem),

---

This work was partly supported by NSF grant DMS 99-88166 and NSA grant MDA 904-99-1-0019.
2000 *Mathematical Subject Classification*: 12F10, 14H30, 20D06, 20E22.

(6) Zassenhaus-Feit-Suzuki Theorem,
(7) Kantor's Rank 3 Theorem (using Buekenhout-Shult's Polar Space Theorem),
(8) Cameron-Kantor's Theorems on Transitive Collineation Groups, and
(9) Liebeck's Orbit Size Theorems (which uses CT).

I shall illustrate how these Recognition Theorems can be used for discovering nice equations whose expected Galois groups are various preassigned nice groups and then for establishing that their Galois groups indeed have the desired values.

History. In my 1957 paper [1], as a bi-product of my Ph. D. Thesis work on resolution of singularities, I discovered that, unlike characteristic zero, in nonzero characteristic p, the affine line is not simply connected, and as examples of this I wrote down the following two families of polynomials

$$Y^n + 1 + \sum_{1=1}^{r} a_i Y^{n_i} \quad \text{and} \quad Y^n + Y + \sum_{1=1}^{r} a_i Y^{n_i}$$

where $a_1, \ldots, a_r$ are polynomials in an indeterminate X, and may be parameters $T, S, \ldots$, with coefficients in a ground field k of characteristic p, and $n > n_1 > \ldots > n_r \geq 0$ are integers such that their differences $n - n_1, \ldots, n - n_r$ are divisible by p, and in the first case n is nondivisible by p whereas in the second case n is divisible by p; note that in both the cases the Y-discriminant of the polynomial is 1. As a special case of the first family. I considered the trinomial

$$Y^{p+t} + XY^t + 1$$

where $t > 0$ is prime to p, and suggested that its Galois group over $k(X)$, as well as the Galois groups of various other members of the two families over $k(X)$ or $k(X, T, \ldots)$, be computed. By an indirect argument concerning this trinomial I showed that as subquotients of the algebraic fundamental group $\pi_A(L_k)$ of the affine line L_k over k we get all finite groups, and this led me to the conjecture that if k is algebraically closed then $\pi_A(L_k)$ consists of all quasi-p groups, i.e., finite groups generated by their p-Sylow subgroups. Here $\pi_A(L_k)$ is defined to be the set of all Galois groups of finite unramified Galois coverings of L_k, and by subquotients of $\pi_A(L_k)$ we mean quotient groups of subgroups of members of $\pi_A(L_k)$. Note that every finite simple group whose order is divisible by p is automatically quasi-p.

At the instigation of Serre, after a gap of thirty years, in 1988, I returned to the calculation of these Galois groups and, following his advice, started learning

group theory for that purpose. Actually, as a college student in Bombay, I was fond of group theory, and wrote to Philip Hall for advice on how to go about solving the odd order problem which I had read in Birkhoff-Maclane's Survey of Modern Algebra. At Hall's suggestion, I was busily reading the papers B. H. and Hanna Neumann, and Reinhold Baer. Then coming to Harvard as a graduate student, I fell under the spell of Oscar Zariski and forgot all about group theory. But when the question of retraining in group theory arose, fortunately I remembered that as a graduate student I was quite friendly with Danny Gorenstein, whom I took to Cornell when I became an assistant professor, and that is how Danny became a group theorist, as I was delayed by a car accident and he was caught by Herstein. At Cornell, I became quite chummy with fellow assistant professor Walter Feit who later on, in collaboration with John Thompson, solved the odd order problem. At any rate, in March 1989, I spent a week with Walter and a week with Danny learning modern group theory. But soon they advised me consult specialists in transitivity like Bill Kantor and Peter Cameron. I was amused to realize that Bill Kantor was a student of Peter Dembowski who was a student of Reinhold Baer, and Peter Cameron was a student of Peter Neumann who is a son of Bernard and Hanna Neumann. What a small world! Perhaps I should add that at Harvard I had taken a course with Richard Brauer who was a friend of Oscar Zariski. I could also mention that in Bombay I studied some group theory with F. W. Levi who was a friend of my father and returned to the Free University of Berlin in 1956. My father S. K. Abhyankar, who was a professor of mathematics in Gwalior, taught me basic mathematics from ancient Sanskrit books, and introduced me to Burnside-Panton's Theory of Equations where I first learnt group theory. This was William Snow Burnside, and not the group theorist William Burnside.

Trinomials. As a result of this retraining in group theory, as reported in my 1992 paper [2], by using CDT, I showed that if k is algebraically closed and $t > 1$ with $(p, t) \neq (7, 2)$ then the Galois group of the above trinomial

$$Y^{p+t} + XY^t + 1$$

is the alternating group A_{p+t}; in case of $(p, t) = (7, 2)$, by using hyperelliptic curves, I showed that it is PSL(2, 8); finally, in case of $t = 1$, by using the Zassenhaus-Feit-Suzuki Theorem, I showed that it is PSL(2, p). For CDT, which gives a complete list of doubly transitive permutation groups, see Cameron [14] or Kantor [18]. For the Zassenhaus-Feit-Suzuki Theorem, which given a complete list of doubly transitive groups in which only the identity fixes three points, see Volume III of Huppert-Blackburn [16]; indeed, for a while in

my travels I carried the three huge volumes of Huppert-Blckburn [16] together with the two big volumes of Suzuki [21], until I became wiser and replaced them with the compact books of Aschbacher [12] and Kleidman-Liebeck [19]. A little later, for $t > 2$, I could replace CDT by Jordan-Margraff Theorems on limits of transitivity which say that if a primitive permutation group is such and such then it must be either the alternating group A_n or the symmetric group S_n. However, from the $t = 2$ case, that is in showing that the Galois group of $Y^{p+2} + XY^2 + 1$ (with $2 \neq p \neq 7$) is A_{p+2}, I have been unable to remove the use of CDT and hence of CT.

Let me note that a small part of the trinomial story, which can be settled by using Burnside's Theorem, turned out to be sufficient to settle the two variable case of Hilbert's 13th problem by giving an example of an algebraic function of two variables which cannot be expressed as a composition of algebraic functions of one variable; see my paper [9] in the Proceedings of the 1995 Franco-Belgian Conference. The said Theorem of Burnside, which has now been generalized into the O'Nan-Scott Theorem, says that a doubly transitive group has a unique minimal normal subgroup, which is either elementary abelian or simple according as whether it is regular or not.

In studying Volume III of Huppert-Blackburn [16], I learnt enough about the Mathieu groups to prove that (as reported in [4] and [5] and partly in collaboration with Popp, Seiler and Yie), assuming k to be algebraically closed and computing Galois groups over $k(X)$, for $p = 3$ the Galois group of $Y^{11} + XY^2 + 1$ is M_{11} and it is isomorphic with the Galois group of $Y^{12} + Y + X$ verifying the fact that M_{11} has a permutation representation of degree 12, and for $p = 2$ the Galois groups of $Y^{23} + XY^3 + 1$ and $Y^{24} + Y^4 + Y + X$ are M_{23} and M_{24} respectively, with similar explicit polynomials having Galois groups M_{22}, M_{12} and $\mathrm{Aut}(M_{12})$ in case of $p = 2$.

Turning to the $t = 1$ case of the above trinomial, i.e., to the trinomial $Y^{p+1} + XY + 1$, the proof using the Zassenhaus-Feit-Suzuki Theorem actually showed that the for any power $q = p^u > 1$ of p, the Galois group of $Y^{q+1} + XY + 1$ over $k(X)$ with k algebraically closed is $\mathrm{PSL}(2, q)$. It took me almost four years to write $Y^{1+q} + XY + 1$ in place of $Y^{q+1} + XY + 1$ which suggested the generalization to the trinomial

$$F^* = F^*(Y) = Y^{\langle m-1\rangle} + XY + (-1)^{\langle m-1\rangle}$$

where we are using the abbreviation

$$\langle i\rangle = 1 + q + q^2 + \ldots + q^i.$$

By replacing Zassenhaus-Feit-Suzuki by Cameron-Kantor's [15] Theorem I on transitive collineation groups, in [3] I showed that

$$\text{Gal}\,(F^*, k(X)) = \text{PSL}\,(m, q)$$

i.e., the Galois group of F^* over $k(X)$ is $\text{PSL}(m, q)$, also for $m > 2$. In [3] I also showed that if we take the X from the coefficient of Y and make it the constant term then the Galois group changes from $\text{PSL}(m, q)$ to $\text{PGL}(m, q)$, i.e.,

$$\text{Gal}\,(F^{**}, k(X)) = \text{PGL}\,(m, q)$$

where

$$F^{**} = F^{**}(Y) = Y^{\langle m-1\rangle} + Y + X.$$

By passing to the vectorial associates of the projective polynomials F^* and F^{**}, i.e., to the polynomials

$$\widehat{\Phi}^* = \widehat{\Phi}^*(Y) = YF^*(Y^{q-1}) = Y^{q^m} + XY^q + (-1)^{\langle m-1\rangle}Y$$

and

$$\widehat{\Phi}^{**} = \widehat{\Phi}^{**}(Y) = YF^{**}(Y^{q-1}) = Y^{q^m} + Y^q + XY$$

we get

$$\text{Gal}\,(\widehat{\Phi}^*, k(X)) = \text{SL}\,(m, q) \quad \text{and} \quad \text{Gal}\,(\widehat{\Phi}^{**}, k(X)) = \text{GL}\,(m, q).$$

Thus the Galois groups of $\widehat{\Phi}^*$ and $\widehat{\Phi}^{**}$ act on an m dimensioanl vector space over $\text{GF}(q)$, whereas the Galois groups of F^* and F^{**} act on the corresponding $m-1$ dimensional projective space over $\text{GF}(q)$, and this is why we call $\widehat{\Phi}^*$ and $\widehat{\Phi}^{**}$ the vectorial associates of the projective polynomials F^* and F^{**}. Actually, this calculation of the Galois groups of F^*, F^{**}, $\widehat{\Phi}^*$ and $\widehat{\Phi}^{**}$, remains valid if instead of assuming k to be algebraically closed we only assume that $\text{GF}(q) \subset k$. Moreover, without any assumption on k, upon letting δ be the unique divisor of u such that

$$\text{Gal}\,(Y^q - Y, k) = Z_\delta$$

where Z_δ is the cyclic group of order δ, it can be shown that

$$\text{Gal}\,(F^{**}, k(X)) = \text{P}\,\Gamma\text{L}_\delta(m, q) \quad \text{and} \quad \text{Gal}\,(\widehat{\Phi}^{**}, k(X)) = \Gamma\text{L}_\delta(m, q)$$

where $\Gamma\text{L}_\delta(m, q)$ is the unique group between $\text{GL}(m, q)$ and $\Gamma\text{L}(m, q)$ such that $\Gamma\text{L}_\delta(m, q)/\text{GL}(m, q) = Z_\delta$ and $\text{P}\Gamma\text{L}_\delta(m, q)$ is the image of $\Gamma\text{L}_\delta(m, q)$

under the canonical epimorphism $\Gamma\mathrm{L}(m,q) \to \mathrm{P}\Gamma\mathrm{L}(m,q)$, and it can also be shown that

$$\mathrm{Gal}\,(F^*, k(X)) \in \mathrm{P}\Gamma\mathrm{SL}_\delta(m,q) \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}^*, k(X)) \in \Gamma\mathrm{SL}_\delta(m,q).$$

where by $\Gamma\mathrm{SL}_\delta(m,q)$ we denote the set of all groups I between $\mathrm{SL}(m,q)$ and $\Gamma\mathrm{L}_\delta(m,q)$ such that $I \cap \mathrm{GL}(m,q) = \mathrm{SL}(m,q) \lhd I$ with $I/\mathrm{SL}(m,q) = Z_\delta$, and by $\mathrm{P}\Gamma\mathrm{SL}_\delta(m,q)$ we denote the set of images of all the members of $\Gamma\mathrm{SL}_\delta(m,q)$ under the canonical epimorphism $\Gamma\mathrm{L}(m,q) \to \mathrm{P}\Gamma\mathrm{L}(m,q)$; it can be shown that $\Gamma\mathrm{SL}_\delta(m,q)$ is a nonempty family which is a complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$ and every I in $\Gamma\mathrm{SL}_\delta(m,q)$ is a split extension of $\mathrm{SL}(m,q)$ such that $\Gamma\mathrm{L}_\delta(m,q)$ is generated by $\mathrm{GL}(m,q)$ and I. Finally, for every divisor d of $q-1$, upon letting $F^{*(d)}$ and $\widehat{\Phi}^{*(d)}$ be obtained by substituting $(-1)^{\langle m-1\rangle}X^d$ for X in F^{**} and $\widehat{\Phi}^{**}$ respectively, i.e., upon letting

$$F^{*(d)} = F^{*(d)}(Y) = Y^{\langle m-1\rangle} + Y + (-1)^{\langle m-1\rangle}X^d$$

and

$$\widehat{\Phi}^{*(d)} = \widehat{\Phi}^{*(d)}(Y) = Y^{q^m} + Y^q + (-1)^{\langle m-1\rangle}X^d Y$$

it can be shown that if $\mathrm{GF}(q) \subset k$ then

$$\mathrm{Gal}\,(F^{*(d)}, k(X)) = \mathrm{PGL}^{(d)}(m,q) \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}^{*(d)}, k(X)) = \mathrm{GL}^{(d)}(m,q)$$

where $\mathrm{GL}^{(d)}(m,q)$ is the unique group between $\mathrm{SL}(m,q)$ and $\mathrm{GL}(m,q)$ such that $\mathrm{GL}(m,q)/\mathrm{GL}^{(d)}(m,q) = Z_d$ and where $\mathrm{PGL}^{(d)}(m,q)$ is the image of $\mathrm{GL}^{(d)}(m,q)$ under the canonical epimorphism $\mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$. Moreover, without any assumption on k it can be shown that

$$\mathrm{Gal}\,(F^{*(d)}, k(X)) \in \mathrm{P}\Gamma\mathrm{L}^{(d)}_\delta(m,q) \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}^{*(d)}, k(X)) \in \Gamma\mathrm{L}^{(d)}_\delta(m,q)$$

where by $\Gamma\mathrm{L}^{(d)}_\delta(m,q)$ we denote the set of all groups J between $\mathrm{SL}(m,q)$ and $\Gamma\mathrm{L}_\delta(m,q)$ such that $J \cap \mathrm{GL}(m,q) = \mathrm{GL}^{(d)}(m,q) \lhd J$ with $J/\mathrm{GL}^{(d)}(m,q) = Z_\delta$ and such that $I < J$ for some $I \in \Gamma\mathrm{SL}^{(d)}_\delta(m,q)$, and by $\mathrm{P}\Gamma\mathrm{L}^{(d)}_\delta(m,q)$ we denote the set of images of all the members of $\Gamma\mathrm{L}^{(d)}_\delta(m,q)$ under the canonical epimorphism $\Gamma\mathrm{L}(m,q) \to \mathrm{P}\Gamma\mathrm{L}(m,q)$; again it can be shown that $\Gamma\mathrm{L}^{(d)}_\delta(m,q)$ is a nonempty family which is a complete set of conjugate subgroups of $\Gamma\mathrm{L}(m,q)$ such that every J in $\Gamma\mathrm{L}^{(d)}_\delta(m,q)$ is a split extension of $\mathrm{GL}^{(d)}(m,q)$ and together with $\mathrm{GL}(m,q)$ generates $\Gamma\mathrm{L}_\delta(m,q)$.

Quintinomials and Sextinomials. Changing m to $2m$ and adding two terms to the trinomial f^* we get the quintinomial

$$F = F(Y) = Y^{\langle 2m-1\rangle} + T^q Y^{\langle m\rangle} + XY^{\langle m-1\rangle} + TY^{\langle m-2\rangle} + 1$$

and its vectorial associate

$$\widehat{\Phi} = \widehat{\Phi}(Y) = YF(Y^{q-1}) = Y^{q^{2m}} + T^q Y^{q^{m+1}} + XY^{q^m} + TY^{q^{m-1}} + Y$$

and in [7], by using Kantor's Rank 3 Theorem [17], I showed that if $\mathrm{GF}(q) \subset k$ then

$$\mathrm{Gal}\,(F, k(X, T)) = \mathrm{PSp}(2m, q) \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}, k(X, T)) = \mathrm{Sp}(2m, q).$$

The said Rank 3 Theorem of Kantor asserts that if the subdegrees of a Rank 3 permutation group coincide with the subdegrees of a classical geometry (symplectic or unitary or orthogonal) then it is a group of automorphisms of such a geometry. Kantor deduces this from the Buekenhout-Shult characterization of polar geometries which in turn is based on the work of Tits [22] on spherical buildings. Actually in [7] I gave the above values of the Galois groups of F and of Φ only under the stronger assumption of k being algebraically closed. That the weaker assumption $\mathrm{GF}(q) \subset k$ is sufficient was later proved in my joint papers [10] and [11] with Paul Loomis where we also considered the deformations of F and $\widehat{\Phi}$ given by

$$F^\sharp = F^\sharp(Y) = Y^{\langle 2m-1\rangle} + T^q Y^{\langle m\rangle} + XY^{\langle m-1\rangle} + S^{q^{m-1}} TY^{\langle m-2\rangle} + S^{\langle m-1\rangle}$$

and

$$\widehat{\Phi}^\sharp = \widehat{\Phi}^\sharp(Y) = YF(Y^{q-1}) = Y^{q^{2m}} + T^q Y^{q^{m+1}} + XY^{q^m} + S^{q^{m-1}} TY^{q^{m-1}} + S^{\langle m-1\rangle} Y$$

and showed that if $\mathrm{GF}(q) \subset k$ then

$$\mathrm{Gal}\,(F^\sharp, k(X, T, S)) = \mathrm{PGSp}(2m, q)$$

and

$$\mathrm{Gal}\,(\widehat{\Phi}^\sharp, k(X, T, S)) = \mathrm{GSp}(2m, q).$$

By adding yet another term we get the sextinomials

$$F^- = F^-(Y) = Y^{\langle 2m-1\rangle} + T^{q^2} Y^{\langle m+1\rangle} + X^q Y^{\langle m\rangle} - XY^{\langle m-2\rangle} - TY^{\langle m-3\rangle} - 1$$

and

$$\Phi^- = \Phi^-(Y) = Y^{q^{2m}} + T^{q^2} Y^{q^{m+2}} + X^q Y^{q^{m+1}} - XY^{q^{m-1}} - TY^{q^{m-2}} - Y$$

and in [8], again by using Kantor's Rank 3 Theorem [17], I showed that if k is algebraically closed then

$$\mathrm{Gal}\,(F^-, k(X, T)) = \mathrm{P}\Omega^-(2m, q) \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}^-, k(X, T)) = \Omega^-(2m, q).$$

Quartinomials. Assuming that $q = q'^2$ where q' is a power of p, and adding only one term we get the quartinomials

$$F^\dagger = F^\dagger(Y) = Y^{\langle 2m-2\rangle} + X^{q'}Y^{\langle m-1\rangle} + XY^{\langle m-2\rangle} + 1$$

and

$$\Phi^\dagger = \Phi^\dagger(Y) = Y^{q^{2m-1}} + X^{q'}Y^{q^m} + XY^{q^{m-1}} + Y$$

and in [6], by using Liebeck's Orbit Size Theorem [20], I showed that if k is algebraically closed then

$$\mathrm{Gal}\,(F^\dagger, k(X)) = \mathrm{PSU}(2m-1, q') \quad \text{and} \quad \mathrm{Gal}\,(\widehat{\Phi}^\dagger, k(X)) = \mathrm{SU}(2m-1, q').$$

REFERENCES

[1] S.S. Abhyankar, *Coverings of algebraic curves,* Amer. J. Math., 79 (1957), pp. 825–856.

[2] S.S. Abhyankar, *Galois theory on the line in nonzero characteristic,* Bull. A.M.S., 27 (1992), pp. 68–133.

[3] S.S. Abhyankar, *Nice equations for nice groups,* Israel J. Math., 88 (1994), pp. 1–24.

[4] S.S. Abhyankar, *Fundamental group of the affine line in positive characteristic,* Proceedings of the 1992 International Colloquium on Geometry and Analysis, Tata Institute of Fundamental Research, Bombay (1995) pp. 1–26.

[5] S.S. Abhyankar, *Mathieu group coverings and linear group coverings,* Contemporary Mathematics, 186 (1995), pp. 293–319.

[6] S.S. Abhyankar, *Again nice equations for nice groups,* Proc. A. M. S., 124 (1996), pp. 2967–2976.

[7] S.S. Abhyankar, *More nice equations for nice groups,* Proc. A. M. S., 124 (1996), pp. 2977–2991.

[8] S.S. Abhyankar, *Further nice equations for nice groups,* Trans. A. M. S., 348 (1996), pp. 1555–1577.

[9] S.S. Abhyankar, *Hilbert's Thirteenth Problem,* Proc. of the Franco-Belgian Conference in Reims, Société Mathématique de France, Séminaires et Congrès 2 (1997), pp. 1–11.

[10] S.S. Abhyankar - P.A. Loomis, *Once more nice equation for nice groups,* Proc. A. M. S., 126 (1998), pp. 1885–1896.

[11] S.S. Abhyankar - P.A. Loomis, *Twice more nice equations for nice groups,* Contemporary Mathematics, 245 (1990), pp. 63–76.

[12] M. Aschbacher, *Finite Group Theory,* Cambridge University Press, 1986.

[13] F. Buekenhout - E.E. Shult, *On the foundations of polar geometry,* Geometriae Dedicata, 3 (1974), pp. 155–170.

[14] P.J. Cameron, *Finite permutation groups and finite simple groups,* Bull. London Math. Soc., 13 (1981), pp. 1–22.

[15] P.J. Cameron - W.M. Kantor, *2-Transitive and antiflag transitive collineation groups of finite projective spaces,* J. of Algebra, 60 (1979), pp. 384–422.

[16] B. Huppert - N. Blackburn, *Finite Groups I, II, III,* Springer-Verlag, 1982.

[17] W.M. Kantor, *Rank 3 characterizations of classical geometries,* J. of Algebra, 36 (1975), pp. 309–313.

[18] W. M. Kantor, *Homogeneous designs and geometric lattices,* J. of Combin. Theory, Ser. A, 38 (1985), pp. 66–74.

[19] P. Kleidman - M. Liebeck, *The Subgroup Structure of the Finite Classical Groups,* Cambridge University Press, 1990.

[20] M. Liebeck, *Characterization of classical groups by orbit sizes,* Proc. A. M. S., 124 (1996), pp. 2961–2966.

[21] M. Suzuki, *Group Theory I, II,* Springer-Verlag, 1986.

[22] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs,* Springer Lecture Notes in Mathematics Number, 386 (1974).

Mathematics Department,
Purdue University,
West Lafayette IN 47907 (USA)
e-mail: ram@cs.purdue.edu