Algebra and Discrete Mathematics
Number 2. **(2009).** pp. 99 – 107

RESEARCH ARTICLE

On Galois groups of prime degree polynomials with complex roots

Oz Ben-Shimol

Communicated by V. I. Sushchansky

Abstract. Let f be an irreducible polynomial of prime degree $p \geq 5$ over $\mathbb{Q}$, with precisely k pairs of complex roots. Using a result of Jens Höchsmann (1999), we show that if $p \geq 4k+1$ then $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to A_p or S_p. This improves the algorithm for computing the Galois group of an irreducible polynomial of prime degree, introduced by A. Bialostocki and T. Shaska.

If such a polynomial f is solvable by radicals then its Galois group is a Frobenius group of degree p. Conversely, any Frobenius group of degree p and of even order, can be realized as the Galois group of an irreducible polynomial of degree p over $\mathbb{Q}$ having complex roots.

1. Introduction

A classical theorem in Galois theory says that an irreducible polynomial f of prime degree $p \geq 5$ over $\mathbb{Q}$ which has precisely one pair of complex (i.e., non-real) roots, has the symmetric group S_p as its Galois group over $\mathbb{Q}$ (see e.g., Stewart[18]). It is natural then to ask the following question: let k be a positive integer and f an irreducible polynomial of prime degree p with precisely k pairs of complex roots. What is its Galois group $\mathrm{Gal}(f/\mathbb{Q})$?. If one tries to imitate the proof of the classical theorem (i.e., the case $k = 1$), one would find, constructively, the subgroup of S_p which is generated by the p-cycle $(1\ 2\ \ldots\ p)$ and an involution $(a_1\ a_2)\cdots(a_{2k-1}\ a_{2k})$. My unsuccessful attempts (so far) to solve the problem in this way indicated that the difference between the degree p

2000 Mathematics Subject Classification: *20B35; 12F12.*

and the number $2k$ of the complex roots, need not be "large" in order to obtain the alternating group A_p at least (i.e., $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to A_p or S_p).

More general observations on such permutation groups brings us to a well-known problem in the theory of permutation groups: let G be a 2-transitive permutation group of degree n which does not contain the alternating group A_n, and let m be its minimal degree. Find the infimum for m in terms of n.

If f is an irreducible polynomial of prime degree p with $k > 0$ pairs of complex roots, where $p > 2k + 1$, then its Galois group $\mathrm{Gal}(f/\mathbb{Q})$ is 2-transitive of degree p, with minimal degree at most $2k$. Therefore, if $B(p)$ is a lower bound for the minimal degree, then $\mathrm{Gal}(f/\mathbb{Q})$ necessarily contains the alternating group A_p when $2k \leq B(p)$. Thus, as $B(p)$ approaches the infimum, the difference $p - 2k$ gets smaller, as required.

Returning to the group-theoretic problem stated above (for degree n, not necessarily a prime), Jordan [10] showed that $B(n) = \sqrt{n-1}+1$ is a lower bound for the minimal degree. A substantial improvement of this bound is due to Bochert [3] who showed that $B(n) = n/8$, and if $n > 216$ then one has an even better bound, namely $B(n) = n/4$. Proofs for the Jordan and Bochert estimates can be found also in Dixon & Mortimor [7], Theorem 3.3D and Theorem 5.4A, respectively. More recently, Liebeck and Saxl [11], using the classification of finite simple groups, have proved $B(n) = n/3$.

Finally, Höchsmann [8], using a concept suggested by W.Knapp which refines the notion of minimal degree in a natural way, namely, *r-minimal degree* $m_r(G)$, where r is a prime divisor of the order of the group G, gave some better estimates, which in the worst case meet Liebeck and Saxl's bounds. Since the group we are dealing with is of prime degree, and we have information about its 2-minimal degree, Hochmann's result serves us better than that of Liebeck and Saxl.

The paper of A.Bialostocki and T.Shaska [2] focuses on the practical aspects of this theoretical problem, in the process of computing the Galois group of prime degree polynomials over $\mathbb{Q}$: 1. The existing techniques, which are mainly based on a theorem of Dedekind (see Cox [6, Theorem 13.4.5]), are expensive and many primes p might be needed in the process. 2. Polynomials in general have plenty of complex roots. 3. Checking whether a polynomial has complex roots is very efficient since numerical methods can be used. Therefore, checking first if the polynomial has complex roots, and then use a "good" bound for the difference between the polynomial's degree and the number of its complex roots, makes the computation of its Galois group much easier. However, they make a use of estimate due to Jordan (summarized in Wielandt [19, page 42]), which

is not sharp at all (as the authors point out in their paper). In fact, Jordan's bound holds for any primitive group of any finite degree - not necessarily 2-transitive of prime degree. In the present paper, we improve their algorithm and discuss some theoretical aspects of the subject.

2. Galois groups of prime degree polynomials with complex roots

A *Frobenius group* is a transitive permutation group which is not regular, but in which only the identity has more then one fixed point. In other words, a Frobenius group G is a transitive permutation group on a set Ω in which $G_\alpha \neq 1$ for some $\alpha \in \Omega$, but $G_\alpha \cap G_\beta = 1$ for all $\alpha, \beta \in \Omega$, $\alpha \neq \beta$. It can be shown that the set of elements fixing no letters of Ω, together with the identity, form a normal subgroup K called the *Frobenius kernel* of G. Frobenius groups are characterized as non-trivial semi-direct products $G = K \rtimes H$ such that no element of $H \setminus \{1\}$ commutes with any element of $K \setminus \{1\}$. Basic examples of Frobenius groups are the subgroups of $\mathrm{AGL}_1(F)$ - the group of the 1-dimensional affine transformations of a field F, i.e. the group consisting of the permutations of the form $t_{\alpha,\beta} : \zeta \mapsto \alpha\zeta + \beta$, $\alpha \in F^*$, $\beta, \zeta \in F$. Clearly, $\mathrm{AGL}_1(F) \cong F \rtimes U$, where U is a non-trivial subgroup of F^*. Identifying U with $\{0\} \rtimes U$, it is easy to verify that no nontrivial subgroup of U is normal in $\mathrm{AGL}_1(F)$. In particular, if $F = \mathbb{F}_p$ - the field of p elements (p prime), then $\mathrm{AGL}_1(p) := \mathrm{AGL}_1(\mathbb{F}_p) \cong \mathbb{F}_p \rtimes U$, where U is a subgroup of $\mathbb{F}_p^*$ (so U is a cyclic of order n, where $n \neq 1$ and n divides $p-1$), is a Frobenius group of degree p. The structure of a Frobenius group of degree $p \geq 5$ is described in the following theorem.

Theorem 2.1. *(Galois)* Let G be a transitive permutation group of prime degree $p \geq 5$, and of order $> p$. Then the following statements are equivalent:
i. G has a unique p-Sylow subgroup.
ii. G is a solvable group.
iii. G is isomorphic to a subgroup of $\mathrm{AGL}_1(p)$.
iv. G is a Frobenius group of degree p.

Proof. See Huppert [9]. □

Let $G \cong \mathbb{F}_p \rtimes U$, U cyclic of order n, $n \neq 1$, $n|p-1$, be a Frobenius group of degree p. Then it is customary to denote $G = F_{pn}$. For example, the dihedral group $D_{2p} = F_{p\cdot 2}$ is a Frobenius group of degree p. The Frobenius groups $F_{p(p-1)}$ appear as Galois groups of the polynomials $X^p - a \in \mathbb{Q}[X]$, where $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^p$. For constructive realization of

Frobenius groups of degree p, see A.A.Bruen, C.Jensen and N.Yui [4].

If f is an irreducible polynomial of degree $p \geq 5$ over $\mathbb{Q}$, then its Galois group $G = \mathrm{Gal}(f/\mathbb{Q})$, as a permutation group acting on the p-set consisting of the p roots of f, is a transitive group of order p (if and only if G contains a p-cycle). Complex conjugation is a $\mathbb{Q}$-automorphism of $\mathbb{C}$ and, therefore, induces a $\mathbb{Q}$-automorphism of the splitting field of f. This leaves the real roots of f fixed, while transposing the complex roots. Therefore, if f has a pair of complex roots, then $|G| > p$. Furthermore, if, in addition, f has more then one real root, then the complex conjugation has more then one fixed point. In particular, G is not a Frobenius group of degree p. By Theorem 1, G is not solvable, thus, f is not solvable by radicals. So we have

Corollary 2.2. Let f be an irreducible polynomial of prime degree $p \geq 5$ over $\mathbb{Q}$, which has a pair of complex roots. If f is solvable by radicals then $\mathrm{Gal}(f/\mathbb{Q})$ is a Frobenius group of degree p, and f has exactly one real root.

Let f be an irreducible polynomial of prime degree $p \geq 5$ and with $k > 0$ pairs of complex roots. By Corollary 2.2, if $p > 2k + 1$ then $G = \mathrm{Gal}(f/\mathbb{Q})$ is not solvable. Our purpose is to show that if $p \geq 4k + 1$ then G contains the alternating group (i.e., G isomorphic to A_p or to S_p).

Theorem 2.3. *(Burnside)* A non-solvable transitive permutation group of prime degree is 2-transitive.

Therefore, a transitive permutation group of prime degree is either 2-transitive or a Frobenius group (see Theorem 2.1).

Proof. See, Burnside [5], or Dixon & Mortimor [7, Corollary 3.5B]. □

Recall that the *minimal degree* $m(G)$ of a permutation group G acting on a set Ω is the minimum of the supports of the non-identity elements: $m(G) := \min\{|\operatorname{supp}(x)| : x \in G, x \neq 1\}$. Hence, G is a Frobenius group if and only if it is a transitive permutation group with minimal degree $|\Omega|-1$, and by Theorem 1, a transitive permutation group of prime degree $p \geq 5$ and of order $> p$ is not solvable if and only if it has minimal degree $< p - 1$.

Now, for every prime divisor r of $|G|$ we define the *minimal r-degree* $m_r(G)$ of G to be the minimum of the supports of the non-identity r-elements (that is, the non-identity elements whose order is a power of r). Using elementary properties of the minimal r-degrees and together with results based on the classification of the finite simple groups, J. Höchsmann [8] has proved

Theorem 2.4. *(Höchsmann)* Let G be a 2-transitive group of degree n which does not contain the alternating group, and let r be a prime divisor of $|G|$. Then
i. $m_r(G) \geq \frac{r-1}{r} \cdot n$ or
ii. $G \geq \mathrm{PSL}(2, 2^m)$, $r = 2^m - 1 \geq 7$ is a Mersenne prime and $m_r(G) = r = n - 2$ or
iii. $G = PSp(2m, 2)$, $n = 2^{m-1} \cdot (2^m - 1)$ with $m > 2$, $r = 2$ and $m_r(G) = \frac{2^{m-1}-1}{2^m-1} \cdot n \geq \frac{3}{7} \cdot n$.
In any case $m_r(G) \geq \frac{r-1}{r+1} \cdot n$.

An immediate consequence (in fact, a special case) of this theorem is

Corollary 2.5. Let G be a 2-transitive group of prime degree p which does not contain the alternating group. Then $m_2(G) \geq \frac{p}{2}$.

Theorem 2.6. Let f be an irreducible polynomial of prime degree $p \geq 5$ over $\mathbb{Q}$. Suppose that f has precisely $k > 0$ pairs of complex roots. If $p \geq 4k + 1$ then $G = \mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to A_p or to S_p. Clearly, if k is odd then $G \cong S_p$.

Proof. Complex conjugation has support $2k$, hence $m_2(G) \leq 2k$. By Corollary 2.2, G is not solvable (f has more than one real root). By Theorem 2.4, G is 2-transitive and, by Corollary 2.5, G necessarily contains the alternating group. □

Therefore, the algorithm given in [2] for computing the Galois group of an irreducible prime degree polynomial, can be improved:

Input: An irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of prime degree p.
Output: The Galois group $\mathrm{Gal}(f/\mathbb{Q})$.
begin
r:=NumberOfRealRoots(f(x));
k:=(p-r)/2;
if $k > 0$ and $p \geq 4k + 1$ then
    if k is odd then
        $\mathrm{Gal}(f/\mathbb{Q}) = S_p$;
    else
        if $\Delta(f)$ is a complete square then
            $\mathrm{Gal}(f/\mathbb{Q}) = A_p$;
        else
            $\mathrm{Gal}(f/\mathbb{Q}) = S_p$;
        endif;
    endif;
else

```
    ReductionMethod(f(x));
endif
end;
```

Remark 2.7. *$\Delta(f)$ denotes the discriminant of $f(x)$. It is well known that if f is a polynomial of degree n with coefficients in a field K, char(K)$\neq$ 2, then $\Delta(f)$ is a perfect square in K if and only if* $\mathrm{Gal}(f/K)$ *is isomorphic to a subgroup of A_n. See e.g., Stewart [18, Theorem 22.7].*

Remark 2.8. *A short discussion on the reduction modulo p method, can be found in [2] and in Cox [6, page 401].*

Remark 2.9. *Corollary 1 in [2] can also be improved: (replace their r with our k - the number of pairs of the complex roots of a given irreducible polynomial of prime degree p). (i) $k = 2$ and $p > 7$. (ii) $k = 3$ and $p > 11$. (iii) $k = 4$ and $p > 13$. (iv) $k = 5$ and $p > 19$.*

3. Non-real realization of F_{pn}

As stated in Corollary 2.2, an irreducible solvable polynomial of prime degree $p \geq 5$ over $\mathbb{Q}$, which has complex roots, has a Frobenius group of degree p (and of even order, of course) as its Galois group over $\mathbb{Q}$. We shall prove that the related "inverse problem" has a positive answer - any Frobenius group of degree p and of even order appears as Galois group of an irreducible polynomial of degree p over $\mathbb{Q}$ having complex roots.

Theorem 3.1. *(Dirichlet)* Let k,h be integers such that $k > 0$ and $(h, k) = 1$. Then there are infinitely many primes in the arithmetic progression $nk + h$, $n = 0, 1, 2, \ldots$.

Proof. See e.g., Serre [15] or Apostol [1]. □

Lemma 3.2. Let l be a positive integer, and let ζ be a primitive l-th root of unity. Then $1, \zeta, \ldots, \zeta^{\varphi(l)-1}$ form a $\mathbb{Z}$-basis for the ring of integers of $\mathbb{Q}(\zeta)$.

Proof. See e.g., Neukirch [12, Chapter I, Proposition 10.2]. □

Lemma 3.3. *(Galois)* Let f be a polynomial of prime degree over $\mathbb{Q}$. Then, f is solvable by radicals if and only if any two distinct roots of f generate its splitting field.

Proof. See Cox [6, Theorem 14.1.1]. □

Theorem 3.4. *(Scholz)* A splitting embedding problem has a proper solution over number fields. (That is, let K be a number field and let M/K be a Galois extension with Galois group H. Suppose that H acts on an abelian group A. Then, there exist a Galois extension L/K which contains M/K such that $\mathrm{Gal}(L/K) \cong A \rtimes H$).

Proof. See Scholz [14]. □

Theorem 3.5. Let F_{pn} be a Frobenius group of degree p and of even order. Then F_{pn} occurs as Galois group of an irreducible polynomial f of degree p over $\mathbb{Q}$ having complex roots. Furthermore, the splitting field of f is $\mathbb{Q}(a, \mathbf{i}b)$ for every complex root $a + \mathbf{i}b$ of f.

Proof. We describe an *explicit* non-real C_n-extensions over $\mathbb{Q}$. By Theorem 3.1, there exist a prime q such that $q \equiv 1(\mod n)$ and $(q-1)/n$ is odd number. Indeed, for every natural number k, write $1 + (2k-1)n = (1-n) + (2n)k$. So, $(1-n, 2n) = 1$ since n is even. Thus, such a prime q does exist. Let m be a primitive root modulo q (that is, a generator of $\mathbb{F}_q^*$). Consider the sum

$$\alpha_n = \zeta_q + \zeta_q^{m^n} + \zeta_q^{m^{2n}} + \ldots + \zeta_q^{m^{\left(\frac{q-1}{n}-1\right)n}}, \tag{1}$$

where ζ_q is a primitive q-th root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is cyclic of order $q-1$ and generated by the automorphism $\sigma : \zeta_q \mapsto \zeta_q^m$. We shall see that $\mathbb{Q}(\alpha_n)/\mathbb{Q}$ is a non-real C_n-extension, and then we shall apply Theorem 3.4.

$\mathbb{Q}(\alpha_n)/\mathbb{Q}$ is a C_n-extension: By the Fundamental Theorem of Galois Theory, it is enough to prove $\mathbb{Q}(\alpha_n) = \mathbb{Q}(\zeta_q)^{\sigma^n}$. The inclusion $\mathbb{Q}(\alpha_n) \subseteq \mathbb{Q}(\zeta_q)^{\sigma^n}$ is because σ^n moves cyclically the summands of (1) (in fact, α_n is the image of ζ_q under the trace map $\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\zeta_q)^{\sigma^n}}$, hence α_n is an element of $\mathbb{Q}(\zeta_q)^{\sigma^n}$). Suppose that $\mathbb{Q}(\alpha_n) \subsetneqq \mathbb{Q}(\zeta_n)^{\sigma_n}$. There exist a proper divisor d of n such that $\mathbb{Q}(\alpha_n) = \mathbb{Q}(\zeta_q)^{\sigma^d}$. In particular, $\sigma^d(\alpha_n) = \alpha_n$, or

$$\sum_{j=0}^{\frac{q-1}{n}-1} \zeta_q^{m^{jn+d}} - \sum_{j=0}^{\frac{q-1}{n}-1} \zeta_q^{m^{jn}} = 0. \tag{2}$$

We shall see in a moment that the summands in (2) are distinct in pairs. Taking it as a fact, there are $2(q-1)/n$ ($\leq q-1$) summands, and dividing each of them by ζ_q gives us a linear dependence among the $1, \zeta_q, \zeta_q^2, \ldots, \zeta_q^{q-2}$ in contradiction to Lemma 1. Now, if $\zeta_q^{m^{jn+d}} = \zeta_q^{m^{in}}$ for some $i, j = 0, 1, \ldots, \frac{q-1}{n} - 1$, $j \geq i$, then $m^{(j-i)n+d} \equiv 1(\mod q)$. m is primitive modulo q so $q-1$ divides $(j-i)n + d$. But, $(j-i)n + d <$

$(\frac{q-1}{n}-1)n+n=q-1$, a contradiction. Therefore, all the summands in (2) are distinct in pairs.

α_n is not real: No summand in (1) is a complex conjugate of the other. Indeed, if $\zeta_q^{m^{jn}} = \zeta_q^{-m^{in}}$ for some $i,j = 0,1,\ldots,\frac{q-1}{n}-1$, $j \geq i$, then $m^{(j-i)n} \equiv -1(\mod q)$, so $m^{2(j-i)n} \equiv 1(\mod q)$. Therefore, the odd number $(q-1)/n$ divides $2(j-i)$, thus divides $j-i$. But $j-i < (q-1)/n$. We conclude that no summand in (1) is a complex conjugate of the other. Finally, if α_n was real, then $\frac{1}{\zeta_q}(\alpha_n - \overline{\alpha_n}) = 0$ and by the same considerations above, we get a contradiction to Lemma 3.2.

Now by Theorem 3.4, we can embed the non-real C_n-extension $\mathbb{Q}(\alpha_n)/\mathbb{Q}$ in a F_{pn}-extension $L/\mathbb{Q}$ (say). Let $\mathbb{Q}(\beta)/\mathbb{Q}$ be an intermediate extension of degree p which corresponds to (the isomorphic copy of) $U \cong C_n$. No non-trivial subgroup of U is normal in F_{pn}, hence $L/\mathbb{Q}$ is the splitting field of the minimal polynomial f of the primitive element β. f is the required polynomial.

If $a+\mathbf{i}b$ is a complex root of f then $L = \mathbb{Q}(a+\mathbf{i}b, a-\mathbf{i}b) = \mathbb{Q}(a,\mathbf{i}b)$ by Lemma 3.3 and Corollary 2.2. □

Remark 3.6. *Any Frobenius group can be realized as Galois group over $\mathbb{Q}$ (the realizations are not necessarily non-real). I.R.Šafarevič [13] proved that any solvable group appears as Galois group over number fields, and J.Sonn [16,17] proved that any non-solvable Frobenius group appears as Galois group over $\mathbb{Q}$.*

Acknowledgment

The author is grateful to Moshe Roitman, Jack Sonn, Tanush Shaska and John Dixon for useful discussions.

References

[1] T.M.Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, 1976.

[2] A.Bialostocki & T.Shaska, *Computing the Galois group of prime degree polynomials with nonreal roots*, Lect. Notes in Computing, **13**, 243-255, (2005).

[3] A.Bochert, *Über die Klasse der Transitiven Substitutionengruppen II.* Math. Ann. **49**, 133-144, (1897).

[4] A.A.Bruen, C.U.Jensen & N.Yui, *Polynomials with Frobenius Groups of Prime Degree as Galois Groups II*, Journal of Number Thoery **24**, 305-359 (1986).

[5] W.Burnside, *Theory of Groups of Finite Order*, Cambridge: at the university press, 1897.

[6] D.A.Cox, *Galois Theory*, Wiley-Interscience, 2004.

[7] J.D.Dixon & B.Mortimor, *Permutation Groups*, Springer-Verlag, 1996.

[8] J.Höchsmann, *On minimal p-degrees in 2-transitive permutation groups*, Archiv der Mathematik, **72**, 405-417, (1999).

[9] B.Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften **134**, Springer-Verlag, 1967.

[10] C.Jordan, *Theoremes sur les groupes primitifs*, J. Math. Pure Appl. **16**, 383-408 (1871).

[11] M.W.Liebeck and J.Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. (3) **63**, 266-314 (1991).

[12] J.Neukirch, *Algebraic Number Theory*, A Series of Comprehensive Studies in Mathematics **322**, Springer-Verlage, 1999.

[13] I.R.Šafarevič, *Construction of fields of algebraic numbers with given solvable Galois groups*, Amer. Math. Soc. Transl. Ser 2 **4**, 185-237, (1956).

[14] S.Scholz, *Über die Bildung algebraisher Zahlkörper mit auflösbarer Galoissche Gruppe*, Math.Z.**30**, 332-356, (1929).

[15] J.P.Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1987.

[16] J.Sonn, *Frobenius Galois groups over quadratic fields*, Israel J. Math. **31**, 91-96 (1978).

[17] J.Sonn, $SL(2,5)$ *and Frobenius Galois groups over* $\mathbb{Q}$, Can. J.Math **32** (2), 281-293 (1980).

[18] I.Stewart, *Galois Theory*, Third Edition, Chapman & Hall/CRC, 2004.

[19] H.Wielant, *Finite permutation groups.* Academic Press, New York-London, 1964.

Contact information

O. Ben-Shimol Department of Mathematics,
University of Haifa,
Mount Carmel 31905, Haifa, Israel
E-Mail: obenshim@math.haifa.ac.il

Received by the editors: 06.09.2008
and in final form 15.04.2009.