FINDING THE GALOIS GROUP OF A POLYNOMIAL: A DEMONSTRATION OF STAUDUHAR'S METHOD

TENGKU MUHAMMAD ANDRI

ABSTRACT. The purpose of this paper is to demonstrate an algorithm to find the Galois group of any monic irreducible polynomial over the field of the rationals with integer coefficients. This algorithm was invented by Richard Stauduhar [15], hence, for the rest it is called the Stauduhar's method. In order to identify the correct subgroup of S_n, several conditions are assumed. Since in every case complex roots, discriminants, and the conjugate values of some functions (to be defined later) must be computed the coefficients of input polynomial must be chosen so there will be relatively small round-off errors. It is further assumed that no two roots are very close to each other and there are no exceptionally large or small roots.

1. HISTORICAL NOTES

The definition of the Galois group itself already implies the course should be taken to solve this problem. Unfortunately, previous methods like one of van der Waerden, demands a factorization of a polynomial of degree $n!$. This method could be described in short as follows:

Let $p(x)$ be the polynomial of degree n over the field Δ (say this is the rational field), and let Σ be the splitting field. We consider the ring $\Sigma(u_1, u_2, \ldots u_n, z)$ of polynomials with coefficients in Δ, in the $(n+1)$ variables $u_1, u_2, \ldots, u_n, z$. From this ring we form the expression

$$\Theta = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

where α_i are the roots of the polynomial (which are in Σ). For each permutation s in the symmetric group S_n, we consider it as a permutation of the variables u_i, and we form the transformed expression $s\Theta$ (e.g if $s = (12)$ then $s = \alpha_1 u_2 + \alpha_2 u_1 + \cdots + \alpha_n u_n$. Finally, we form the product F of all the expressions $z - s\Theta$ for all $s \in S$. Now F is a symmetric function of the α_i, and hence, can be expressed in terms of elementary symmetric function of the α_i. These are precisely the coefficients of $p(x)$, and in fact lie in Δ. So F is actually in the smaller ring $\Delta(u_1, u_2, \ldots, u_n)$. We decompose F into irreducible factors $F_1 F_2, \ldots, F_n$ in this ring, and we apply the permutations s as above to the resulting equation

$$F = F_1 F_2 \cdots F_n.$$

Now, for an arbitrary factor (say F_1), those permutations which carry this factor into itself form a group which is isomorphic to the galois group of the given equation.

Later, with the help of electronic computers, Zassenhaus and Cockayne put this method into more practice. However, this method doesn't compute the Galois group in all cases but leaves us with several choices. The advantages of this method is that the same program could be used for different values of n. In order to demonstrate this method the effective version of Tchabotareff density function is used.

The software MAPLE computes the Galois group of monic irreducible polynomials over infinite or finite fields, It computes the Galois group of polynomials up to degree seven. This software based on the works of L. Soicher, J. McKay, and Butler which in turn based on the van der Waerden's method.

Stauduhar's method, on the other hand, uses only the basic facts about galois group and will certainly give a single solution to the input polynomial provided that minimum accuracy of the roots is attained.

2. OVERVIEW OF THE METHOD

In order to find the galois group of an irreducible monic polynomial with integer coefficients this method makes use of the complex roots of the given polynomial. Hence these roots are computed first and are placed in an initial ordering $r_1, r_2, \ldots, r_n$. Let Γ be the galois group of $p(x)$ with respect to this ordering. Suppose M is a maximal transitive subgroup of S_n, $M \neq A_n$, and $[S_n : M] = k$. To determine if Γ is a subgroup of M, or some conjugate of M, we calculate a resolvent polynomial of degree k, $Q_{(S_n,M)}(y)$ numerically, using a function $F(x_1, x_2, \ldots, x_n)$ belonging to M in S_n, and a set $\pi_1, \pi_2, \ldots, \pi_k$ of right coset representatives for M in S_n.

This resolvent is monic with integer coefficients (see theorem). It is tested for integer roots. If it has none, then Γ is not contained in any of the conjugates of M, and similar resolvents may be computed, corresponding to other conjugacy classes of maximal transitive subgroups of S_n.

Suppose $Q_{(S_n,M)}(y)$ has an integer root. Then this root is $\pi_i F(r_1 r_2, \ldots r_n)$ where π_i is one of the coset representatives, and hence, Γ is a subgroup of $\pi_i M \pi_i^{-1}$.

The roots of $p(x)$ now is reordered so that $r'_j = r_{\pi_i(j)}$. After the reordering, according to theorem, Γ is a subgroup of M.

Assuming that Γ is a subgroup of M, let M^* be a maximal transitive subgroup of M, and F^* is a function belonging to M^* in M. The resolvent polynomial $Q_{(M,M^*)}(y)$ of degree $[M : M^*]$ is computed, and this new polynomial is tested for integer roots. If an integer root of $Q_{(M,M^*)}$ is found, the roots of $p(x)$ are once again reordered to ensure that Γ is a subgroup of M^*.

The search is continued in this way until either none of the resolvents at a given level give an integer root or a minimal transitive subgroup of S_n is located. At each level of searching, only groups not previously eliminated is considered. For example, if S_n has maximal subgroups M_1 and M_2, and it is discovered that $Q_{(S_n,M_1)}$ has no integer roots, but $Q_{(S_n,M_2)}$ does, so Γ is not a subgroup of M_1, and Γ is a subgroup of M_2, then groups which lie within the intersection of M_1 and M_2 are ruled out as the candidates for Γ.

It is further assumed that those integer roots of resolvents with respect to which reordering is taking place are not repeated roots. In the case the integer roots of a resolvent have multiplicity greater than one, the resolvent can be calculated with respect to a new function.

The discriminant D^2 is used in two ways. First, if none of the resolvents associated with the maximal transitive subgroup of S_n yield an integer root, then $\Gamma = A_n$ or $\Gamma = S_n$ depending on whether D^2 is a perfect square (van der Waerden's theorem). Second, if D^2 is a square, and we have determined that Γ is a subgroup of M then Γ is a subgroup of the intersection of M and A_n. This will simplify the search procedure.

2.1. **Ordering of the roots.** Let $p(x)$ be a monic irreducible polynomial over the rationals. Let K be the splitting field of Let G be the group of all field automorphisms fixing the rationals. Let $s \in G$, then

$$s(r_k) = r_{s(k)} = r_{i_k}$$

$$r_k \xrightarrow{s} r_{i_k}$$

$$k \longrightarrow i_k$$

Hence, whenever the galois group is given as a group of permutation of n letters, an ordering of the roots is also given, and vice versa. This happens because we have freedom to label the subgroups of S_n.

Let $+V_4$ be our example,

$$\begin{array}{ccc} 1 & — & 2 \\ | & & | \\ 4 & — & 3 \end{array}$$

generators: $(14)(23), (12)(34)$, or,

$$\begin{array}{ccc} 1 & — & 2 \\ | & & | \\ 3 & — & 4 \end{array}$$

generators: $(13)(24), (12)(34)$.

Let the first be the initial ordering $1, 2, 3, 4$. Then the second ordering comes out as the result of mapping (34) works on $1, 2, 3, 4$. So, if the galois group is $+V4$ under the first ordering, then under the second ordering it is

$$(34)V_4(34)^{-1}.$$

2.2. **Function belongs to a subgroup of S_n.** Let $F(x_1, x_2, \ldots, x_n)$ be a function of n indeterminate.

Let G be a group of permutations of n letters. If F is unchanged by precisely the permutations of G we say that F belongs to G. Such functions are constructible.

Let $F^*(x_1x_2, \ldots x_n) = x_1x_2^2 \cdots x_n^n$. $F = \sum_{\sigma \in G} \sigma F * (x_1x_2, \ldots x_n)$ where

$$\sigma F(x_1, x_2, \ldots, x_n) = F(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

This function belongs to G.

EXAMPLE. For $n = 3$, the function

$$\begin{aligned} F &= x_1x_2^2x_3^3 + x_2x_3^2x_1^3 + x_3x_2^2x_2^3 \\ &= x_1x_2x_3(x_2x_3^2 + x_3x_1^2 + x_1x_2^2). \end{aligned}$$

(Note: $x_1x_2x_3$ is a constant)

$$F' = x_2x_3^2 + x_3x_1^2 + x_1x_2^2$$

belongs to A_3.

Particularly for any alternating groups A_n, a function of the form

$$D^2 = \Pi_{i<j}(x_i - x_j)^2$$

belongs to A_n.

Given the function $F(x_1x_2, \ldots, x_n)$ and a permutation $\pi \in S_n$, the function $\pi F(x_1, x_2, , \ldots, x_n)$ is called the conjugate function or the conjugate value of the function $F(x_1, x_2, \ldots x_n)$.

Let H be a subgroup of S_n. Let F belong to G in S_n. Then F takes exactly $[H : H^G]$ distinct conjugate values under the permutations of H, exactly those of $G' = G^H$ leave unchanged. Suppose G and H are subgroups of S_n, G is in H, and F belong to G in H. Then for $\pi \in H$, πF belongs to $\pi G \pi^{-1}$ in H.

2.3. **Generating the polynomial resolvents.** Let $p(x) \in Q[x]$, monic, irreducible with integral coefficients. Let $r_1, r_2, \ldots, r_n$ be the initial ordering of the roots.

Let H be a transitive subgroup of S_n. Suppose with respect to this ordering, Γ the galois group of $p(x)$ is a subgroup of H. For any G in H and F, a function belonging to G, let $\pi_1, \pi_2, \ldots \pi_k$, be the set of coset representatives w.r.t H, then

$$Q_{(H,G)}(y) = \Pi_{i=1}^k (y - \pi_i(F(r_1, r_2, \ldots, r_n))$$

is called the resolvent polynomial of G with respect to H and having integral coefficients.

$F(r_1, r_2, \ldots, r_n)$ is a root of of $Q_{(H,G)}(y)$ since the identity (e) is one of coset representatives.

Theorem 2.1. *If $F(r_1, r_2, \ldots, r_n)$ is not a repeated root of $Q_{(H,G)}(y)$ then Γ is a subgroup of G if and only if $F(r_1, r_2, \ldots, r_n)$ is an integer.*

Theorem 2.2. *Assume $\pi_i(F(r_1, r_2, \ldots r_n))$ is not a repeated root of $Q_{(H,G)}(y)$; then Γ is a subgroup of $\pi_i G \pi^{-1}$ if and only if*

$$\pi_i F(r_1, r_2, \ldots, r_n) \text{ is an integer.}$$

Theorem 2.3. *Then if Γ is a subgroup of $\pi_i G \pi_i^{-1}$ and is not a repeated root of $Q_{(H,G)}(y)$ under a new ordering*

$$r'_j = r_{\pi_i(j)'}$$

Γ is a subgroup of G.

The following theorem is useful to simplify our search:

Theorem 2.4 (van der Waerden). *Let $p(x)$ be irreducible, monic polynomial of degree n with integral coefficients. If the discriminant D^2 is a perfect square then the galois group is a subgroup of the alternating group.*

Note: perfect square means integer, or $\sqrt{D^2} \in \mathbb{Q}$.

3. How to apply theorems and result

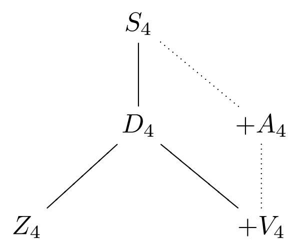
For polynomials of degree three van der Waerden's theorem is used to determine the galois group. If the discriminant D^2 is a perfect square then the Galois group is $+A_n$, otherwise it is S_n, since the only candidates for it are $+A_3$ and S_3.
EXAMPLE. Let $p(x) = 1 + x + x^3$.

$$r_1 = 0.341163901914 + 1.1615414i$$
$$r_2 = 0.341163901914 - 1.1615414i$$
$$r_3 = -0.682327803828$$

$D^2 = -31$ (not a square) Then the Galois group is full, S_3.
EXAMPLE. Let $p(x) = -1 - 2x + x2 + x3$.

$$r_1 = -7.80193773581$$
$$r_2 = 1.24697960372$$
$$r_3 = -0.445041867913$$

$D^2 = 49$ (a perfect square). Then the galois group is the alternating group A_3. For polynomials of degree four, a simplified form of the lattice of S_4, which is called a search tree, is needed.



If D^2 is not a perfect square, then $+A_4$ and $+V_4$ are ruled out. The search starts form the left. If the polynomial resolvent $Q_{(S_4,D_4)}$ gives an integer root and not a repeated root then the galois group Γ is a subgroup of D_4 under a suitable ordering. If Γ is also a subgroup of Z_4 then $\Gamma = Z_4$ since Z_4 is a minimal transitive subgroup in S_4. If Γ is not a subgroup of D_4 then $\Gamma = S_4$. If Γ is a subgroup of D_4 but not of Z_4 then $\Gamma = D_4$. In case D^2 is a perfect square, S_4, D_4, and Z_4 are ruled out. The candidates are $+A_4$ and $+V_4$. We check whether Γ is a subgroup of D_4, if it is, then $\Gamma = +V_4$, if it is not then $\Gamma = +A_4$.
EXAMPLE. Let $p(x) = 1 + x4$. Initial ordering of the roots:

$$\begin{cases} r_1 = -0.707106781186 + 0.707106781186i \\ r_2 = -0.707106781186 - 0.707106781186i \\ r_3 = 0.707106781186 + 0.707106781186i \\ r_4 = 0.707106781186 - 0.707106781186i \end{cases}$$

$D^2 = 256$ (a perfect square). The candidates are $+A_4$ and $+V_4$. If Γ is also a subgroup of D_4 then $\Gamma = +V_4$. To decide whether this is the case we compute $\pi_i F$ for every coset representative of D_4 with respect to S_4

$$F = \sum_{\sigma \in D_4} x_{\sigma(1)} x_{\sigma(2)}^2 \cdots x_{\sigma(4)}^4$$

after cancelling constant factors we get

$$F = x_1x_3 + x_2x_4$$

(see Appendix Two).

The coset representatives of D_4 with respect to S_4 are $\{(e), (23), (34)\}$ (see Appendix Three). So,

$$(e)F = -2$$
$$(23)F = 2$$
$$(34)F = 0$$

Since at least one of the conjugate values of F give an integer root then the galois group of $p(x) = 1 + x^4$ is $+V_4$.

For polynomials of degree five the search tree is as follows:

$$\begin{tikzcd}
S_5 \arrow[d, dash] \arrow[dr, dash, dotted] & \\
F_{20} \arrow[d, dash] & +A_5 \arrow[dl, dash, dotted] \\
+D_5 \arrow[d, dash] & \\
+Z_5 &
\end{tikzcd}$$

Suppose D^2 is not a perfect square, then Γ is not one of these: $+A_5, +D_5, +Z_5$. The remaining candidates of Γ are S_5 and F_{20}. Computing the polynomial resolvent of F_{20} with respect to S_5 we could decide whether Γ is a subgroup of F_{20} or not. If Γ is a subgroup of F_{20} then $\Gamma = F_{20}$. If none of the conjugate functions give an integer then Γ is not a subgroup of F_{20}, in this case the galois group Γ is full, the symmetric group S_5.

Suppose D^2 is a perfect square, then the candidates for ΓF are $+A_5, +D_5, +Z_5$. Hence there is no need to find out whether Γ is a subgroup of F_{20} or not. We proceed further to find out whether Γ is a subgroup of $+D_5$ or not. If it is, then we check whether it is a subgroup of $+Z_5$. If once again Γ is a subgroup of $+Z_5$ then $\Gamma = +Z_5$ since $+Z_5$ is a minimal subgroup and in fact the only minimal transitive subgroup of the search tree. If Γ is not a subgroup of $+Z_5$ but it is a subgroup of $+D_5$ then $\Gamma = +D_5$. If Γ is not a subgroup of $+D_5$ then $\Gamma = +D_5$.

EXAMPLE. Let $p(x) = 2 + x5$.

$$\begin{cases} r_1 = -1.148698355 \\ r_2 = -0.354967313105 + 1.09247705578i \\ r_3 = -0.354967313105 - 1.09247705578i \\ r_4 = 0.929316490603 + 0.67518795240i \\ r_5 = 0.929316490603 - 0.67518795240i \end{cases}$$

$D^2 = 50000$ (not a perfect square).

$$F = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2.$$

$$\begin{aligned} (e)F &= 10.7605967409 - 33.1177114395i \\ (12)(34)F &= -28.1716080068 + 20.467871299i \\ (12435)F &= 0 \\ (15243)F &= 10.7605967409 + 33.1177114395i \\ (12453)F &= 34.8220225319 \\ (12543)F &= -28.1716080068 - 20.4678712992i \end{aligned}$$

Since $(12435)F$ is an integer then Γ is a subgroup of F_{20} under the new ordering

$$\begin{cases} r_1 = 0.929316490603 - 0.6751879524i, \\ r_2 = -1.148698355, \\ r_3 = 0.929316490603 + 0.6751879524i \\ r_4 = -0.354967313105 + 1.09247705578i \\ r_5 = -0.354967313105 - 1.092477055781i \end{cases}$$

Conclusion: $\Gamma = F_{20}$.

EXAMPLE. Let $p(x) = 1 + x + x^5$.

Initial ordering:

$$\begin{cases} r_1 = 0.877438833123 + 0.74486176662i \\ r_2 = 0.877438833123 - 0.74486176662i \\ r_3 = -0.500000000000 + 0.8660254037841 \\ r_4 = -0.500000000000 - 0.8660254037841 \\ r_5 = -0.754877666247 \end{cases}$$

$D^2 = 3381$ (not a perfect square).

$$F = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2.$$

$$(e)F = 14.1901768507 + 21.9903048657i$$
$$(12)(34)F = 14.1901768507 - 21.9903048657i$$
$$(12435)F = -6.62872926169 + 12.263503695i$$
$$(15243)F = 0.030963071708$$
$$(12453)F = 24.8461417502$$
$$(12543)F = -4.55952615721 - 3.69442145371i$$

None of the conjugates give an integer, then Γ is not a subgroup of F_{20}. $\Gamma = S_5$.

EXAMPLE. $p(x) = 12 - 5x + x^5$.

Initial ordering:

$$\begin{cases} r_1 = -1.84208596619 \\ r_2 = -0.351854240828 + 1.70956104337i \\ r_3 = -0.351854240828 - 1.70956104337i \\ r_4 = 1.27289722392 + 0.7197986681484i \\ r_5 = 1.27289722392 - 0.7197986681484i \end{cases}$$

$D^2 = 64000000$ (a perfect square).

$$F = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2$$

$$eF = 0.621045428367 - 145.295693239i$$
$$(12)(34)F = -3.08195506973 - 1.36227509475i$$
$$(12435)F = 100$$
$$(15243)F = 0.024236798106$$
$$(12453)F = -150.633163828 - 92.6277364613i$$
$$(12543)F = 0.621045428367 + 145.295693239i$$

Hence, Γ is a subgroup of $(12435)F_{20}(12435)^{-1}$, since Γ is also a subgroup of A_5 then Γ is a subgroup of $F_{20}\&A_5 = D_5$. The roots are reordered:

$$\begin{cases} r_1 = 1.27289722392 - 0.7197986681484i \\ r_2 = -1.84208596619 \\ r_3 = 1.2728922392 + 0.7197986681484i \\ r_4 = -0.351854240828 + 1.70956104337i \\ r_5 = -0.351854240828 - 1.70956104337i \end{cases}$$

The following function belongs to Z_5:

$$F = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x4x_5^2 + x_5x_1^2$$
$$eF = -5 - 15.8113883008i$$
$$(35)(12)F = -5 + 15.8113883008i$$

Since none of the conjugate values of F gives an integer, then Γ is not a subgroup of Z_5. $\Gamma = +D_5$.

EXAMPLE. $p(x) = 1 + 3x - 3x^2 - 4x^3 + x^4 + x^5$.

Initial ordering of the roots:

$$\begin{cases} r_1 = -1.91898594723 \\ r_2 = 1.68250706566 \\ r_3 = -1.30972146789 \\ r_4 = 0.830830026004 \\ r_5 = -0.284629676546 \end{cases}$$

$D^2 = 14641$ (a perfect square).

$$F = (x_1x_2 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2.$$

$$(e)F = 70.9219146335$$
$$(12)(34)F = 64.5554503713$$
$$(12435)F = 1.07701459367$$
$$(15243)F = 95.6627758542$$
$$(12543)F = 0$$

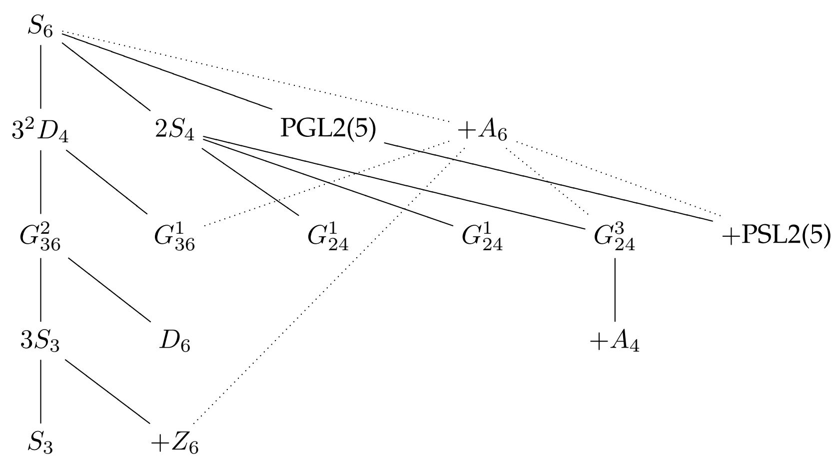
Hence Γ is a subgroup of F_{20} and since it is also a subgroup of A_5 then Γ is a subgroup of D_5. The new ordering:

$$r_1 = -1.30972146789$$
$$r_2 = -1.91898594723$$
$$r_3 = 0.830830026004$$
$$r_4 = -0.284629676546$$
$$r_5 = 1.68250706566$$

The following function belongs to Z_5:

$$F = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + x_5x_1^2$$
$$(e)F = -4$$
$$(12)(35)F = 8$$

Hence, $\Gamma = Z_4$. For polynomials of degree six the search tree:



Suppose D^2 is a perfect square, then the candidates are:

$$+G_{36}^1, +Z_6, +G_{24}^3, +A_4, +\text{PSL2(5)}, \text{ and } +A_6.$$

The search starts from the left. If Γ is a subgroup of 3^2D_4 then $\Gamma = +G_{36}^1$. If it is not, we proceed to the second left branch of the tree. If Γ is a subgroup of $2S_4$ then there are two possibilities: $+G_{24}^3$ and $+A_4$. If Γ is a subgroup of $+A_4$ then $\Gamma = +A_4$. If it is not then $\Gamma = +G_{24}^3$. If Γ is not a subgroup of $2S_4$ we proceed to PGL2(5). If Γ is a subgroup of PGL2(5) then $\Gamma =$ +PSL2(5). If it is not then $\Gamma = +A_6$. Similar procedure is applied for D^2 is not a square.

For polynomials of degree seven, the search tree:

$$\begin{tikzcd}
S_7 \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
A_7 \arrow[r, dotted, dash] & +\mathrm{PSL}(2) \arrow[d, dash] & F_{42} \arrow[d, dash] \\
& +F_{21} \arrow[d, dash] & D_7 \\
& +Z_7 &
\end{tikzcd}$$

Suppose D^2 is a perfect square then the candidates are $A_7, +$PSL3(2)$, +F_{21}$, and Z_7. If Γ is a subgroup of +PSL3(2) then A_7 is ruled out. If Γ is not a subgroup of F_{21} then $\Gamma = +$PSL3(2). If it is then we proceed further to find out whether it is a subgroup of $+Z_7$. If it is then $\Gamma = +Z_7$. Suppose D^2 is not a perfect square. Then the candidates are S_7, F_{42}, and D_7. If Γ is a subgroup of F_{42} then S_7 is ruled out. If Γ is a subgroup of D_7 then $\Gamma = D_7$. It is important to notice that in each level of searching the roots are reordered.

APPENDIX ONE

Transposition. Transposition is a mapping of the form (ij) where $i, j \in N$, the set of n letters.
Even permutations. An even permutation is a permutation consists of even number of transpositions, e.g $(ij)(\ell k)$ is an even permutation, where $i, j, k, \ell \in N$.
Proposition. A mapping $\sigma \in S_n$ could be represented in an infinitely many ways as product of transpositions.
Proposition. If n is even, the rotation of n side polygon is always odd, other wise, if n is odd the rotation is even.

$$(1234) = (12)(13)(14)$$

while

$$(12345) = (12)(13)(14)(15).$$

Hence, if n is even Z_n, is not a subgroup of A_n, while in case n is odd, Z_n is a subgroup of A_n.
Proposition. The set of all even permutations of S_n forms a group, the alternating group A_n.
Transitivity. A subgroup G of S_n is transitive whenever for any $i, j \in N$, there exists a mapping $\sigma \in G$ such that $\sigma(i) = j$, e.g., for $n \geq 3$, Z_2 is not transitive, Z_n is always transitive, D_n is always transitive.

APPENDIX TWO

Degrees	Group	Contained in	Function	Generators
4	D_4	S_4	$x_1x_3+x_2x_4$	(1234), (13)
4	Z_4	D_4	$x_1x_2^2+x_2x_3^2+x_3x_4^2+x_4x_1^2$	(1234)
4	$+V_4$	–	–	(12)(34), (13)(24)
5	F_{20}	S_5	$(x_1x_2+x_2x_3+x_3x_4+x_4x_5+x_5x_1$ $-x_1x_3-x_3x_5-x_5x_2-x_2x_4-x_4x_1)^2$	(1234)
5	$+D_5$	–	–	(12345),(25),(34)
5	$+Z_5$	$+D_5$	$x_1x_2^2+x_2x_3^2+x_3x_4^2+x_4x_5^2+x_5x_1^2$	(12345)
6	3^2D_4	S_6	$x_1x_2x_3+x_4x_5+x_6$	(123),(456),(12),(45),(14)(25)(36)
6	$+G_{36}^1$	–	–	(123),(456),(12)(45),(1425)(36)
6	$+G_{36}^2$	3^2D_4	$(x_1-x_2)(x_2-x_3)(x_3-x_1)$ $(x_4-x_5)(x_5-x_6)(x_6-x_4)$	(123),(456),(12)(45),(1425)(36)
6	$3S_3$	G_{36}^2	$(x_1-x_2)(x_2-x_3)(x_3-x_1)$ $(x_4-x_5)(x_5-x_6)(x_6-x_4)$	(123),(456),(14)(25)(36)
6	D_6	G_{36}^2	$(x_1x_4+x_2x_5+x_3x_6)$	(123)(456),(12)(45),(14)(25)(36)
6	S_3	$3S_3$	$x_1x_4+x_2x_6+x_3x_5$	(123)(456),(1425)(36)
6	Z_6	$3S_3$	$x_1x_6^2+x_2x_4^2+x_3x_5^2$ $+x_4x_2^2+x_5x_1^2+x_6x_2^2$	(123)(456),(14)(25)(36)
6	$2S_4$	S_6	$x_1x_2+x_3x_4+x_5x_6$	(12),(34),(56)(135),(246),(13)(24)
6	G_{24}^1	$2S_4$	$(x_1+x_2-x_3-x_4)$	(12)(34)
			$(x_3+x_4-x_5-x_6)$	(34)(56)
			$(x_5-x_6-x_1-x_6)$	(12)(56)
			(x_1-x_2)	(135)(246)
			$(x_3-x_4)(x_5-x_6$	(14)(23)(56)
6	G_{24}^2	$2S_4$	$(x_1+x_2-x_3-x_4)$	(12)(34)(56)
			$(x_3+x_4-x_5-x_6)$	(34)(56),(56)
			$(x_5+x_6-x_1-x_2)$	(135)(246)
6	$+S_4/V_4$	$2S_4$	–	(135)(246),(13)(24),(12)(34),(34)(56)
6	$+A_4$	$+S_4/V_4$	see G_{24}^2	(12)(34),(34)(56),(12)(56),(135),(246)
6	PGL2(5)	S_6	$(x_1x_2+x_3x_5+x_4x_6)$	(126)(354),
			$(x_1x_3+x_4x_5+x_2x_6)$	(2354)
			$(x_3x_4+x_1x_6+x_2x_5)$	
			$(x_1x_5+x_2x_4+x_3x_6)$	
6	+PSL2(5)			(126)(354), (12345), (2354)
7	+PSL3(2)	S_7	$x_1x_2x_4+x_1x_3x_7+x_1x_5x_6$ $+x_2x_3x_5+x_2x_6x_7+x_3x_4x_6+x_4x_5x_7$	(1234567), (235)(476),(2743)(56)
7	F_{42}	S_7	$x_1x_2x_4+x_1x_2x_6+x_1x_3x_4+x_1x_3x_7$ $+x_1x_5x_6+x_1x_5x_7+x_2x_3x_5+x_2x_3x_7$ $+x_2x_4x_5+x_2x_6x_7+x_3x_4x_6+x_3x_5x_6$ $+x_4x_5x_7+x_4x_6x_7$	(1234567), (243756)
7	$+F_{21}$	+PSL3(2)	see $F_{42}\preceq S_7$	(1234567),(235)(476)
7	D_7	F_{42}	$x_1x_2+x_2x_3+x_3x_4$ $x_4x_5+x_5x_6+x_6x_7+x_7x_1$	(1234567), (27)(45)(36)
7	$+Z_7$	$+F_{21}$	see $D_7\preceq F_{42}$	(1234567)

APPENDIX THREE

Degree four	Coset representatives
D_4 in S_4	e,(23),(34)
Z_4 in D_4	e,(12)(34)
Degree five	Coset representatives
F_{20} in S_5	e,(12)(34),(12345),(15243),(12453),(12543)
Z_5 in $+D_5$	e, (12)(35)
Degree six	Coset representatives
3^2D_4 in S_6	e,(2543),(236)(45),(25436),(25)(34),(2453),(25),(2345),(24536),((3645)
G^2_{36} in 3^2D_4	e,(56))
$3S_3$ in 3^2D_4	e,(12)(45),(56),(12)(465)
S_3 in $3S_3$	e,(123),(132)
Z_6 in $3S_3$	e,(123),(132)
D_6 in 3^2D_4	e,(123),(132),(56),(123)(56),(132)(56)
$2S_4$ in S_6	e,(24635),(26)(35),(345),(2345),(253),(345),(256)(34),(26435),(2346) (234),(25)(36),(2435),(24)(35),(26543)
G^1_{24} in $2S_4$	e,(12)
G^2_{24} in $2S_4$	e,(13)(24)
$+A_4$ in $+S_4/V_4$	e,(13)(24)
PGL2(5) in S_6	e,(13),(123),(132),(12)

REFERENCES

[1] Butler, G.,& McKay, J., The Transitive Groups up to Order Eleventh, Communications in Algebra, 11 (8), 863–911 (1983)

[2] Cayley, A.,*On the Substitution Groups of Six,Seven, and Eight Letters*, Quart. J. Pure Appl. Math., v.25, 71–88, 137–155, 1891

[3] Foulkes, H. O.,*The resolvent of an Equation of Seventh Degree*, Quart. J. Math Oxford Series (2), 9–19 1931

[4] Girtsmair, K.,*On Root Polynomials of Cyclic Cubic Equations*, Archive of Mathematics, 36, No.4, 313–326, 1970

[5] Jacobson, N. *Lectures in Abstract Algebra*, v.3.D. van Nostrand Co., Princeton, New Jersey, 1964

[6] Kappe, L. C.,& Warren, B.,*An Elementary Test for the Galois Group of Quartic Polynomials*,

[7] Lefton, P.,*Galois Resolvent of Permutation Groups*, American Mathematical Monthly, 84, 642–644, 1977

[8] van der Linden, F. J., *The Computation of Galois Groups*, Compu. Methods in Number Theory, Part II, Math Centre Tract 155 199–211, 1982

[9] Maurer,W. D.,*The Use of Computer in Galois Theory*, Computational Problems in Abstract Algebra,J.Leech(ed.), Pergamon Press, 325–326, 1970

[10] McKay, J.,*Some remarks on Computing Galois Groups*, SIAM J. Computing 8, 1407–1445, 1979

[11] Rotman, J.,*Galois Theory*, Springer-Verlag, 1990

[12] utherford, D. E., *Substitutional Analysis*, The Edinburg University Press,London, 1948

[13] Soicher, L.,*Computing Galois Groups over The nationals*, Journal of Number Theory, 20, 273–281, 1985

[14] ims,Charles,*Computatonal Methods in the Study of Permutation Groups*, Compu.Problems in Abstract Algebra, (Proc.Conf., Oxford,1967), 169–183, Pergamon Press, Oxford 1970

[15] Stauduhar, R.,*The Determination of Galois Groups*, MathlCompu. 27 981–996, 1973

[16] Stewart, Ian,*Galois Theory*, Chapman, & Hall, London 1973

[17] van der Waerden, B. L.,*Modern Algebra*, Frederick Ungar Publishing Co., New York, 1953.

KOLEJ UNIVERSITI TEKNOLOGI TUN HUSSEIN ONN
E-mail address: t_andri@yahoo.com