Comm. Korean Math. Soc. **11** (1996), No. 1, pp. 23-31

ON THE GALOIS GROUPS OF THE SEPTIC POLYNOMIALS

GEON-NO LEE

ABSTRACT. Our main purpose in this paper is to determine the Galois group of the given irreducible septic polynomial over **Q** by using three resolvant polynomials and the discriminant of the given polynomial.

1. Introduction

Computer determination of the Galois groups of irreducible polynomial with integer coefficient has been described by many authors. ([1],[2]) The Galois group can naturally be considered as a subgroup of S_n, the symmetric group on n letters. We need at first to classify transitive subgroup of S_n up to conjugacy. There are seven types of transitive subgroup of S_7 ; the cyclic group C_7 of order 7, the dihedral group D_7 of order 14, the metacyclic group M_{21} of order 21, the affine transformation group $Aff(1,7)$ of order 42, the projective special linear group $PSL(3,2)$ of order 168, the alternating group A_7 of order 2520, the symmetric group S_7 of order 5040. The classification of S_n has been solved up to $n = 15$. ([3],[5]) In this paper we determine the Galois group of irreducible septic polynomials over **Q** using 3 resolvants of degree 21, 35 and 42, respectively. These three resolvant polynomial are very simple to implement on a personal computer. Many other resolvants can be found in the literature. ([1],[2],[4],[5])

2. Solvable Galois groups of septic polynomial

In this section we shall determine all possible Galois group of an irreducible septic polynomial over **Q** which are solvable.

Received February 11, 1995. Revised December 8, 1995.
1991 AMS Subject Classification: Primary 11R32; Secondary 11R09.
Key words and phrases: Galois group, Resolvant polynomial, Solvable group.

THEOREM 1.1. *Let p be a prime number and let G be a transitive subgroup of S_p. The following conditions are equivalent :*

1. *G is solvable.*
2. *G has only one p-Sylow subgroup.*
3. *G is isomorphic to a subgroup of $Aff(1,p)$ containing the translations.*

PROOF. $(1 \Rightarrow 2)$ Let H be a minimal normal subgroup of G. Since p is prime, G is primitive, so H is transitive. Since G is solvable, H is abelian. Thus H is of order p, and H is the only p-Sylow subgroup G.

$(2 \Rightarrow 3)$ Let C be a cyclic subgroup of order p of S_p. Then G can be regarded as a subgroup of $N_{S_p}(C)$, the normalizer of C. S_p has $(p-2)!$ subgroups of order p. So the order of $N_{S_p}(C)$ is equal to $p(p-1)$. Note that $Aff(1,p)$ has the same order. We can easily check $N_{S_p}(C) \cong Aff(1,p)$.

$(3 \Rightarrow 1)$ Let T be the subgroup of translations. Then T is normal and G/T is cyclic of order d, with $d|p-1$. Thus we have a monomorphism $G/T \to GL(1,p)$ and $GL(1,p) \cong F_p^*$. T and G/T are solvable, so G is solvable. □

The transitive solvable permutation group of degree p are classified by the divisors d of $p-1$. G can be identified with

$$< \sigma, \tau : \sigma^p = 1, \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^r >,$$

where r is of order d in $(Z/pZ)^*$. We can conclude

COROLLARY 1.2. *If G is a solvable Galois group of an irreducible septic polynomial over $\mathbf{Q}$, then G is isomorphic to one of the following 4 subgroups of S_7 :*

$$\begin{aligned} \langle (1\ 2\ 3\ 4\ 5\ 6\ 7) \rangle &\cong C_7 \\ \langle (1\ 2\ 3\ 4\ 5\ 6\ 7),\ (2\ 7)(3\ 6)(4\ 5) \rangle &\cong D_7 \\ \langle (1\ 2\ 3\ 4\ 5\ 6\ 7),\ (2\ 3\ 5)(4\ 7\ 6) \rangle &\cong M_{21} \\ \langle (1\ 2\ 3\ 4\ 5\ 6\ 7),\ (2\ 4\ 3\ 7\ 5\ 6) \rangle &\cong Aff(1,7). \end{aligned}$$

3. The non-solvable Galois group of S_7

In this section we shall determine all possible Galois group of an irreducible septic polynomial over $\mathbf{Q}$ which are non-solvable.

PROPOSITION 2.1. *Let G be a non-solvable Galois group of an irreducible septic polynomial over $\mathbf{Q}$. If $|S_7 : G| < 7$, then $G = S_7$ or A_7.*

PROOF. Since G is transitive, G has a 7-cycle Thus we may assume that the 7-cycle is $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. If G contains any 2-cycle, then $G = S_7$. If G does not contain any 2-cycle, we consider the following cosets of G in S_7.

$G_1 = (1\ 2)\ G,\ G_2 = (2\ 3)\ G,\ G_3 = (3\ 4)\ G,\ G_4 = (4\ 5)\ G,$
$G_5 = (5\ 6)\ G,\ G_6 = (6\ 7)\ G,\ G_7 = (7\ 1)\ G.$

Here $|S_7 : G| < 7$, so there exists i, j such that $G_i = G_j$ and $i \neq j$.

Suppose $G_1 = G_2$, then

$G_3 = (3\ 4)\ G = \sigma(2\ 3)\sigma^{-1}\ G = \sigma(2\ 3)G\ \sigma^{-1} = \sigma G_2\sigma^{-1} = \sigma G_1\sigma^{-1}$
$= \sigma(1\ 2)G\sigma^{-1} = \sigma(1\ 2)\sigma^{-1}G = (2\ 3)\ G = G_2.$

Similarly, $G_3 = G_4$, $G_4 = G_5$, $\cdots$. So, $G_1 = G_2 = G_3 = \ldots = G_7$.

Similarly, we can show that if there exist i, j such that $G_i = G_j$ and $i \neq j$, then $G_1 = G_2 = \cdots = G_7$. Thus we have

$(1\ 2)\ G = (2\ 3)\ G \implies (1\ 2)(2\ 3) = (1\ 2\ 3) \in G.$
$(2\ 3)\ G = (3\ 4)\ G \implies (2\ 3)(3\ 4) = (2\ 3\ 4) \in G.$
$(3\ 4)\ G = (4\ 5)\ G \implies (3\ 4)(4\ 5) = (3\ 4\ 5) \in G.$
$(4\ 5)\ G = (5\ 6)\ G \implies (4\ 5)(5\ 6) = (4\ 5\ 6) \in G.$
$(5\ 6)\ G = (6\ 7)\ G \implies (5\ 6)(6\ 7) = (5\ 6\ 7) \in G.$

The 3-cycles $(1\ 2\ 3)$, $(2\ 3\ 4)$, ... , $(5\ 6\ 7)$ generate A_7.

Consequently, we proved that if G does not contain any 2-cycle, then $G = A_7$. □

PROPOSITION 2.2. *Let G be a transitive non-solvable subgroup of A_7. If G has any 3-cycle, then $G = A_7$.*

PROOF. Without loss of generality, we can assume that G has the 3-cycle $\tau = (1\ 2\ t)$ and $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$.

We can easily verify that

$\langle (1\ 2\ 3), \sigma \rangle = \langle (1\ 2\ 4), \sigma \rangle = \ldots = \langle (1\ 2\ 7), \sigma \rangle$

Thus G has (1 2 3), (1 2 4), $\cdots$, (1 2 7), and these generate A_7.
Therefore, $G = A_7$. □

PROPOSITION 2.3. *Let G be a transitive non-solvable subgroup of S_7 and let $G^+ = G \cap A_7$. If $|A_7 : G^+| < 7$, then $G = S_7$ or A_7.*

PROOF. We will show this proposition by using Proposition 2.2.
Since G is transitive, G^+ is also transitive.
If G^+ has any 3-cycle, then $G^+ = A_7$ and so $G = S_7$ or $G = A_7$.
Suppose G^+ does not contain any 3-cycle.
Consider the following cosets of G^+ in A_7.
$H_1 = (1\ 2\ 3)\ G^+$, $H_2 = (2\ 3\ 4)\ G^+$, $H_3 = (3\ 4\ 5)\ G^+$,
$H_4 = (4\ 5\ 6)\ G^+$, $H_5 = (5\ 6\ 7)\ G^+$, $H_6 = (6\ 7\ 1)\ G^+$,
$H_7 = (7\ 1\ 2)\ G^+$.
But $|A_7 : G^+| < 7$, then there exist i and j such that, $H_i = H_j$ and $i \neq j$. By the similar computation of Proposition 2 1, we have
$H_1 = H_2 = \cdots = H_7$.
$(1\ 2\ 3)\ G^+ = (2\ 3\ 4)\ G^+$ implies $(1\ 2\ 3)(2\ 3\ 4)^{-1} = (1\ 2\ 4) \in G^+$.
But it is a contradiction. So, G^+ has 3-cycles and $G^+ = A_7$.
Therefore, $G = S_7$ or A_7. □

PROPOSITION 2.4. *Let G be a transitive non-solvable subgroup of S_7 and $G^+ = G \cap A_7$. Then $|A_7 : G^+| = 7$ is impossible.*

PROOF. If G has only even permutations, then $G \subset A_7$ so $G = G^+$. Otherwise G has an odd permutation σ. Let $\phi : G \to G$ be a mapping defined by $\phi(g) = \sigma g$. Then ϕ is well-defined and a bijective mapping, so G has same number of even permutations as odd permutations. Therefore, $|G : G^+| = 1$ or 2. The order of G^+ is devided by 7. (7 divides the order of G) Therefore, $|A_7 : G^+| = 7$ is impossible. □

PROPOSITION 2.5. *Let G be a transitive non-solvable subgroup and let $G^+ = G \cap A_7$. If $|A_7 : G^+| \geq 8$, then G^+ does not contain a subgroup of order 60.*

PROOF. If $|A_7 : G^+| \geq 8$, then $|G^+| \leq 360$. Since $7 || G^+|$ we have $|G^+| \leq 315$. Suppose G^+ contains a subgroup of order 60, then $|G^+| =$ 60, 120, 180, 240, or 300. But 7 devides the order of G^+. So, G^+ has not a subgroup of order 60. □

THEOREM 2.6. *If G is a non-solvable Galois group of an irreducible septic polynomial over* $\mathbf{Q}$, *then G is isomorphic to one of the following three subgroups of S_7 : S_7, A_7 or $<(1\ 2\ 3\ 4\ 5\ 6\ 7),\ (2\ 6)(3\ 4)> \cong PSL(3,2) \cong PSL(2,7)$.*

PROOF. Let G be a non-solvable Galois group of an irreducible septic polynomial over $\mathbf{Q}$ and let $G^+ = G \cap A_7$. Then G^+ is also not solvable. If G^+ is not isomorphic to S_7 or A_7, then the order of G^+ is smaller than 316.

Consider the non-solvable simple groups of order less than 316. The first non-abelian simple group is isomorphic to A_5 of order 60. But, A_5 is not transitive in S_7 and G^+ does not contain a subgroup of order 60. So, A_5 cannot be a non-solvable Galois group of an irreducible septic polynomial. The second simple group is $PSL(3,2) \cong PSL(2,7)$ of order 168. Note that $<(1234567),\ (26)(34)> \cong PSL(3,2)$. So, G^+ can be isomorphic to $PSL(3,2)$.

Suppose $PSL(3,2)$ is a nontrivial subgroup of G^+ . Then the order of G^+ is devided by 168, but it is not possible. The third simple group is A_6. But this order is already 720. So, G^+ cannot be isomorphic to A_6, by Proposition 2.3, 2.4 and 2.5. □

4. Determination of the Galois group

Let $f(x)$ be an irreducible polynomial of degree 7 over $\mathbf{Q}$, θ_i roots of $f(x)$ in C, and let G be the Galois group of $f(x)$ over $\mathbf{Q}$. Let

$$f_2(x) = \prod_{i<j}^{7}(x - (\theta_i + \theta_j)).$$

$$f_3(x) = \prod_{i<j<k}^{7}(x - (\theta_i + \theta_j + \theta_k)).$$

$$f_4(x) = \prod_{i\neq j}^{7}(x - \theta_i(\theta_i + \theta_j)).$$

Then the degree of $f_2(x)$, $f_3(x)$ and $f_4(x)$ are 21, 35 and 42 respectively.

Considering the action of G on the set of the roots of $f(x)$, we obtain the following theorems.

THEOREM 3.1. *$f_2(x)$ is reducible over $\mathbf{Q}$ if $G \cong C_7$ or D_7 and $f_2(x)$ is irreducible, otherwise.*

THEOREM 3.2. *$f_3(x)$ is reducible over $\mathbf{Q}$ if $G \cong C_7$, D_7, M_{21}, $Aff(1,7)$ or $PSL(3,2)$ and $f_3(x)$ is irreducible, otherwise.*

THEOREM 3.3. *Let df be the discriminant of the polynomial $f(x)$. Then df is a square in $\mathbf{Q}$ if and only if $G \cong C_7$, M_{21}, $PSL(3,2)$ or A_7.*

THEOREM 3.4. *$f_4(x)$ is reducible over $\mathbf{Q}$ if $G \cong M_{21}$. $f_4(x)$ is irreducible if $G \cong PSL(3,2)$.*

Summarizing these results together we have the following table.

	$f_2(x)$	$f_3(x)$	$f_4(x)$	df
C_7	reducible	reducible		square
D_7	reducible	reducible		not square
M_{21}	irreducible	reducible	reducible	square
$Aff(1,7)$	irreducible	reducible		not square
$PSL(3,2)$	irreducible	reducible	irreducible	square
A_7	irreducible	irreducible		square
S_7	irreducible	irreducible		not square

THEOREM 3.5. *If $f(x) = x^7 - a$, $a \in \mathbf{Q}$ is irreducible over $\mathbf{Q}$, then the Galois group of $f(x)$ is $Aff(1,7)$.*

PROOF. The Galois group of $f(x)$ is solvable and of order 42.
Thus the Galois group of $f(x)$ must be $Aff(1,7)$. □

5. Examples

EXAMPLE 4.1. The Galois group of $f(x) = x^7 - 7x + 3$ is the projective special linear group $PSL(3,2)$.

Let θ_i be the roots of given polynomial $f(x)$, where

$\theta_1 = -1.4443022027143747159153549821233486740 59$
$\theta_2 = -0.7556610338813547080394271428845448652 91 -$

$1.20612825938812030712739842286539024191 8\ i$

θ_3 = Complex Conjugate of θ_2

$\theta_4 = 0.42895317162492626614752091423895842174 87$

$\theta_5 = 0.61666312264252632215997392307893826075 73 -$
$1.21158033992379146394358477338799087714 8\ i$

θ_6 = Complex Conjugate of θ_5

$\theta_7 = 1.29334485356710522152674050749560346137 8$

Then the followings hold.

$f_2(x) = 27 + 567\ x + 3969\ x^2 + 9261\ x^3 - 2601\ x^7 + 630\ x^8 - 2597\ x^9 - 171\ x^{14} + 175\ x^{15} + x^{21}$
and $f_2(x)$ is irreducible over $\mathbf{Q}$.

$f_3(x) = -31104 + 36288\ x + 1227744\ x^2 - 2222640\ x^3 - 12446784\ x^4 + 29042496\ x^5 - 592029\ x^7 + 4975614\ x^8 - 9345672\ x^9 + 1393266\ x^{10} - 12357947\ x^{11} + 978750\ x^{14} + 1139292\ x^{15} + 408366\ x^{16} + 1739696\ x^{17} + 34452\ x^{21} - 56826\ x^{22} - 79086\ x^{23} + 906\ x^{28} - 280\ x^{29} + x^{35}$

$f_3(x) = (\ 9 - 21\ x - 42\ x^2 + 14\ x^4 + x^7\ )\ (\ -3456 - 4032\ x + 110880\ x^2 - 7056\ x^3 - 876624\ x^4 + 1154832\ x^5 - 1568784\ x^6 + 1674299\ x^7 - 1497363\ x^8 + 1472415\ x^9 - 956137\ x^{10} + 760116\ x^{11} - 487452\ x^{12} + 293706\ x^{13} - 179421\ x^{14} + 62538\ x^{15} - 51345\ x^{16} + 14700\ x^{17} - 10668\ x^{18} + 588\ x^{19} - 1176\ x^{20} + 897\ x^{21} - 63\ x^{22} + 42\ x^{23} - 14\ x^{25} + x^{28}\ )$

$f_3(x)$ is reducible over $\mathbf{Q}$.

$f_4(x) = 531441 + 66134880\ x^4 + 558104904\ x^5 - 8944181190\ x^6 + 34130322\ x^7 + 3173417919\ x^8 - 22299191460\ x^9 + 86366483847\ x^{10} - 199606243410\ x^{11} + 197550882585\ x^{12} + 32713649010\ x^{13} - 69094856925\ x^{14} + 56002955148\ x^{15} + 9944980416\ x^{16} - 12445617114\ x^{17} - 4194399699\ x^{18} + 1652866236\ x^{19} - 1586446344\ x^{20} - 2336527836\ x^{21} + 156521484\ x^{22} - 147503034\ x^{23} - 92001513\ x^{24} + 5205060\ x^{25} - 16953804\ x^{26} + 20907908\ x^{27} + 216351\ x^{28} - 1205694\ x^{29} + 1618274\ x^{30} + 18144\ x^{32} + 35672\ x^{33} + 1026\ x^{35} + 2597\ x^{36} + 14\ x^{39} + x^{42}$

$f_4(x)$ is irreducible over $\mathbf{Q}$.

$\sqrt{df} = 194481$. So, df is a square.

$f_2(x)$ is irreducible over $\mathbf{Q}$, $f_3(x)$ is reducible over $\mathbf{Q}$, $f_4(x)$ is irreducible over $\mathbf{Q}$ and df is a square. Thus the Galois group is $PSL(3,2)$.

EXAMPLE 4.2. The Galois group of $f(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$ is the cyclic group C_7.

$f_2(x)$ is reducible over $\mathbf{Q}$, $f_3(x)$ is reducible over $\mathbf{Q}$ and df is a square.

Thus the Galois group is C_7.

EXAMPLE 4.3. The Galois group of $f(x) = x^7 + 7x^3 + 7x^2 + 7x - 1$ is the dihedral group D_7.

$f_2(x)$ is reducible over $\mathbf{Q}$, $f_3(x)$ is reducible over $\mathbf{Q}$ and df is not a square.

Thus the Galois group is D_7.

EXAMPLE 4.4. The Galois group of $f(x) = x^7 - 14x^5 + 56x^3 - 56x + 22$ is the metacyclic group M_{21}.

$f_2(x)$ is irreducible over $\mathbf{Q}$, $f_3(x)$ is reducible over $\mathbf{Q}$, $f_4(x)$ is reducible over $\mathbf{Q}$ and df is a square.

Thus the Galois group is M_{21}.

EXAMPLE 4.5. The Galois group of $f(x) = x^7 - 2$ is the affine transformation group $Aff(1,7)$.

$f_2(x)$ is irreducible over $\mathbf{Q}$, $f_3(x)$ is reducible over $\mathbf{Q}$ and df is not a square.

Thus the Galois group is $Aff(1,7)$.

EXAMPLE 4.6. The Galois group of $f(x) = x^7 + 7x^4 + 14x + 3$ is the alternating group A_7 .

$f_2(x)$ is irreducible over $\mathbf{Q}$, $f_3(x)$ is irreducible over $\mathbf{Q}$ and df is a square.

Thus the Galois group is A_7.

EXAMPLE 4.7. The Galois group of $f(x) = x^7 + 2x + 2$ is the symmetric group S_7 .

$f_2(x)$ is irreducible over $\mathbf{Q}$, $f_3(x)$ is irreducible over $\mathbf{Q}$ and df is not a square.

Thus the Galois group is S_7.

References

1. R. P. Stauduhar, *The Determination of Galois groups*, Math. Comp. **27** (1973), 981-996.
2. L. Soicher and J. Mckay, *Computing Galois groups over rationals*, J. Number Th. **20** (1985), 273-281.

3. G. Butler and J. Mckay, *The transitive groups of degreeup to eleven*, Comm. in Alg. **11** (1983), 863 - 911.
4. K. Girstmair, *On invariant polynomials and their applications in field theory*, Math. Comp. **48** (1987), 781-797.
5. H. Cohen, *A course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

Department of Mathematics
Korea University
Seoul 136-701, Korea