Tôhoku Math. Journ.
22(1970), 670-678.

GALOIS GROUP OF AN EQUATION $X^n - aX + b = 0$

KÔJI UCHIDA

(Received Sep. 8, 1970)

Let k be a field, and let a and b be indeterminates. In the following we want to determine the Galois group of an equation

$$(1) \qquad X^n - aX + b = 0 .$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of this equation, and let $K = k(a, b, \alpha_1, \alpha_2, \cdots, \alpha_n)$. The Galois group G of K over $k(a, b)$ is considered as a permutation group of $(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Let p be the characteristic of k. If $p = 0$, G is known to be a symmetric group S_n [4, Corollary 2]. More generally we prove

THEOREM 1. *If the characteristic p is not a divisor of $n(n-1)$, G is equal to S_n.*

When p is a divisor of n or $n-1$, we have not succeeded to determine G except $n = p^m$ or $n = p^m + 1$ (Theorem 2). But we have some interesting examples. Above notations are used throughout this paper.

1. Let D be the discriminant of the equation (1). Then it holds [4, p. 222]

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2}(n^n b^{n-1} - (n-1)^{n-1} a^n) .$$

LEMMA 1. *G is doubly transitive.*

PROOF. The equation (1) is irreducible over $k(a, b)$. If α is a root of (1),

$$\frac{X^n - \alpha^n}{X - \alpha} = a$$

is irreducible over $k(a, b, \alpha) = k(a, \alpha)$. So G is doubly transitive.

Now we prove Theorem 1. As G is primitive by the above lemma, it suffices to show that G contains a transposition [5, Theorem 13. 3]. In the field $k(a, b)$ we consider $k(a)$ as a constant field. Then D is prime in $k(a)(b)$, and it is ramified in $k(a, b, \alpha_1)$ or also in K, because

$$D = \{(\alpha_1 - \alpha_2) \cdots (\alpha_1 - \alpha_n)\}^2 \{(\alpha_2 - \alpha_3) \cdots (\alpha_{n-1} - \alpha_n)\}^2 .$$

We determine the inertia group of D. We put

$$f(X) = X^n - aX + b .$$

As

$$Xf'(X) - nf(X) = (n-1)aX - nb ,$$

g. c. d. of $f(X)$ and $f'(X) = nX^{n-1} - a$ mod D is equal to $(n-1)aX-nb$. Namely there exists a factorization

$$f(X) \equiv ((n-1)aX - nb)^2 \bar{f}_2(X) \cdots \bar{f}_r(X) \pmod{D} ,$$

where $\bar{f}_i(X)$ are prime to $(n-1)aX-nb$ mod D. Let $k(a, b)_D$ be the completion of $k(a)(b)$ by D. Then $f(X)$ is split as

$$f(X) = f_1(X) f_2(X) \cdots f_r(X)$$

in $k(a, b)_D$ by Hensel's lemma, where $f_1(X)$ is of degree 2 and $f_i(X) \equiv \bar{f}_i(X)$ (mod D) for $i \geqq 2$. Let K_D be a completion of K by some divisor of D. Then as

$$K_D = k(a, b)_D(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

and as $f_i(X) = 0$ for $i \geqq 2$ generate unramified extensions of $k(a, b)_D$, the inertia group of D is generated by the transposition of the roots of $f_1(X) = 0$. Then G contains a transposition, so the proof of Theorem 1 is completed.

COROLLARY 1. *If the characteristic p is odd or if n is odd, the Galois group of an equation*

$$X^n + aX^2 + bX + c = 0 \tag{2}$$

is equal to S_n, where a, b and c are indeterminates.

PROOF. If p is not a divisor of $n(n-1)$, this is shown by specializing a to

0. If p is a divisor of $n-1$, we specialize b to 0. We can show similarly to the proof of the theorem that the Galois group of the equation

$$X^n + aX^2 + c = 0$$

is a symmetric group S_n. This time we consider the ramification of prime c in $k(a)(c)$. Now if p is not 2 and p is a divisor of n, p is not a divisor of $(n-1)(n-2)$. Then the Galois group of

$$X^{n-1} + aX + b = 0$$

is a symmetric group S_{n-1}. If we consider $k(a, b)$ as a constant field of $k(a, b, c)$, residue field extension mod c has Galois S_{n-1} .Then the Galois group of (2) contains a transposition.

COROLLARY 2. *Let k be any field and let a, b, c and d be indeterminates. Then the Galois group over $k(a, b, c, d)$ of an equation*

$$X^n + aX^3 + bX^2 + cX + d = 0 \tag{3}$$

is a symmetric group S_n.

PROOF. If the characteristic p of k is not 2, or if n is odd, assertion follows from Corollary 1. If $p=2$ and n is even, the residue class field extension mod d is obtained by the equation

$$X^{n-1} + aX^2 + bX + c = 0 .$$

Then its Galois group contains a transposition by Corollary 1, so the Galois group of (3) is a symmetric group.

2. In this section we deal with the case $n=p^m$ or $n=p^m+1$.

THEOREM 2. *Let k be a field of characteristic p. Let F be a finite field with p^m elements, and ζ be a primitive (p^m-1)-st root of unity.*

(A) *If $n=p^m$ in the equation (1) , the Galois group G is isomorphic to the group of the transformations of F of type*

$$x \to cx^s + d ,$$

where $c(\neq 0)$ and d are elements of F and s is an automorphism of F which fixes the elements of $k\cap F$.

(B) *If $n=p^m+1$, the Galois group is isomorphic to the group of the transformations of projective space $P_1(F)$ of type*

$$(x_0, x_1) \rightarrow (cx_0^s + dx_1^s, ex_0^s + fx_1^s),$$

where c, d, e and f are elements of F such that $cf-de\neq 0$, and s is as above.

PROOF. (A) Let α and β be two roots of (1). Then from

$$\alpha^{p^m} - a\alpha + b = 0$$

and

$$\beta^{p^m} - a\beta + b = 0,$$

it follows that

$$(\alpha-\beta)^{p^m-1} = a.$$

Therefore K is equal to $k(\alpha, \beta, \zeta)$. Now let γ be any root of (1) and we put

$$x_\gamma = \frac{\gamma-\alpha}{\beta-\alpha}.$$

This runs over F when γ runs over the roots of (1). Let σ be an element of G. Then the transformation

$$x_\gamma \rightarrow x_{\sigma(\gamma)}$$

is given by

$$x_\gamma \rightarrow ax_\gamma^s + b.$$

Here

$$a = \frac{\beta^\sigma-\alpha^\sigma}{\beta-\alpha}, \quad b = \frac{\alpha^\sigma-\alpha}{\beta-\alpha},$$

and s is the restriction of σ on F. The degree of K over $k(a,b)$ is equal to $p^m(p^m-1)\cdot[k(\zeta):k]$. Hence all transformations of this type are obtained by the elements of G.

(B) Let α, β and γ be three roots of (1). It follows that

$$a=\frac{\gamma^{p^m+1}-\alpha^{p^m+1}}{\gamma-\alpha}=\frac{\gamma^{p^m+1}-\beta^{p^m+1}}{\gamma-\beta}.$$

Then it holds

$$\alpha(\gamma^{p^m-1}+\alpha\gamma^{p^m-2}+\cdots+\alpha^{p^m-1})=\beta(\gamma^{p^m-1}+\beta\gamma^{p^m-2}+\cdots+\beta^{p^m-1}),$$

which is equivalent to

$$\alpha(\gamma-\alpha)^{p^m-1}=\beta(\gamma-\beta)^{p^m-1}$$

or

$$\left(\frac{\gamma-\beta}{\gamma-\alpha}\right)^{p^m-1}=\frac{\alpha}{\beta}.$$

As the right hand side is independent of γ, the ratio

$$\frac{\delta-\beta}{\delta-\alpha}:\frac{\gamma-\beta}{\gamma-\alpha}$$

represents an element of $F\cup\{\infty\}$ for any root δ of (1). So

$$y_\delta=\left(\frac{\delta-\beta}{\delta-\alpha},\frac{\gamma-\beta}{\gamma-\alpha}\right)$$

becomes a homogeneous coordinate of $P_1(F)$. The transformation

$$y_\delta\to y_{\sigma(\delta)},\ \sigma\in G$$

is equal to the transformation

$$y_\delta\to\begin{pmatrix}c\ d\\ e\ f\end{pmatrix}y_\delta^s,$$

where

$$\begin{pmatrix}c\ d\\ e\ f\end{pmatrix}\sim\begin{pmatrix}(\alpha-\gamma)(\alpha^\sigma-\beta)(\beta^\sigma-\gamma^\sigma) & (\alpha-\gamma)(\beta-\beta^\sigma)(\alpha^\sigma-\gamma^\sigma)\\ (\alpha-\alpha^\sigma)(\gamma^\sigma-\beta^\sigma)(\beta-\gamma) & (\alpha-\beta^\sigma)(\alpha^\sigma-\gamma^\sigma)(\beta-\gamma)\end{pmatrix}$$

As the extension degree $[K:k(a,b)]=[k(\alpha,\beta,\gamma,\zeta):k(a,b)]$ is equal to the number of the transformations of this type, (B) is proved.

3. In the case which are not included in the preceding argument, it seems too difficult to determine G. There exists another special case.

PROPOSITION 1. *When the characteristic $p=2$ and $n=2^m-1$, G is a subgroup of $GL(m,2)=PSL(m,2)$.*

PROOF. The roots of (1) and 0 make an abelian group of type $(2,2,\cdots,2)$, because they are the roots of

$$X^{2^m}-aX^2+bX=0\,.$$

As every element of G induces an automorphism of this group, G is contained in $GL(m,2)$.

When $n=7$, G is equal to $GL(3,2)$. But we do not know whether $G=GL(m,2)$ in general or not. When $p\neq 2$, following proposition shows whether G contains an odd permutation or not.

PROPOSITION 2. *When $p\neq 2$, the discriminant D is square only in the following cases:*

(i) $4p|n$ *or* $4p|n-1$

(ii) $2p|n$ *or* $2p|n-1$, *and* -1 *is square in* k.

PROOF. Obvious from the form of D.
We now give some examples for small n.

EXAMPLES. (i) Galois groups are symmetric groups S_n or alternating groups A_n in the following cases:

$p=2$, $n=10$, 11, 12, 13 or 14
$p=3$, $n=6$ or 7
$p=5$, $n=10$ or 11.

These are examined by specializing a and b to elements of the ground field.

(ii) When $p=2$ and $n=6$, the Galois group is isomorphic to A_5 if the ground field contains the cubic roots of unity. If we put α and β two roots of

$$X^6 - aX + b = 0,$$

then

$$X^6 - aX + b = (X-\alpha)(X-\beta)(X^2+(\alpha+\beta)\zeta X+\alpha^2+\beta^2+\alpha\beta\zeta)$$
$$\times (X^2+(\alpha+\beta)\zeta^2 X+\alpha^2+\beta^2+\alpha\beta\zeta^2)$$

holds, where $\zeta^2+\zeta+1=0$. If γ is a root of third factor of right hand side,

$$\delta = \alpha + \beta\zeta + \gamma\zeta$$

is a root of fourth factor. Hence K is equal to $k(\alpha, \beta, \gamma)$. Then it holds

$$[K:k(a,b)] = [k(\alpha,\beta,\gamma):k(a,b)] = 60.$$

As the Galois group is not solvable (all the doubly transitive solvable groups are known by Huppert [2, or 3. Chap. III-19]), it is isomorphic to A_5.

(iii) If $p=3$ and $n=12$, the Galois group is isomorphic to Mathieu group M_{11}. We have a factorization

$$(3) \quad X^{12} - aX + b = (X^6+cX^4+dX^3-c^2X^2+cdX-d^2-c^3)$$
$$\times (X^6-cX^4-dX^3-c^2X^2+cdX-d^2+c^3)$$

for $a=-cd^3, b=d^4-c^5$. As c and d are polynomials of the roots, $k(c,d)$ is contained in K. If we show $G \cong M_{11}$ in the case $k=F_3$ is a prime field, it holds in general as M_{11} is a simple group. From now on we assume that k is a prime field. We will determine the order of the Galois group G. It is easily shown that $[k(c,d): k(a,b)]=22$. Now we consider the first factor in the right hand side of (3). It is irreducible over $k(c,d)$, and it is factorized into the factors of degree 1 and degree 5 when $c=d=1$. Then its Galois group is doubly transitive, and it is not solvable. As its determinant is equal to c^6d^6, the Galois group is isomorphic to A_6 or A_5. Two factors of (3) have same Galois group, as they are transposed by $(c,d)\to(-c,-d)$. Therefore the Galois group of K over $k(c,d)$ is isomorphic to one of $A_6\times A_6$, $A_5\times A_5$, A_6 and A_5. Sylow 5-groups of $A_6\times A_6$ and $A_5\times A_5$ are of order 5^2. Then Sylow 5-groups of G are Sylow 5-groups of S_{12}. Hence G contains a 5-cycle, and G contains A_{12} [5, Theorem 13.9]. But the above argument shows that G does not contain any element of order 7. It is a contradiction. Therefore the Galois group of K over $k(c,d)$ is isomorphic to A_6 or A_5. Then the order of G is equal to

$$(\mathrm{I}) \quad 22\times(A_6:1) = 22\cdot 6\cdot 5\cdot 4\cdot 3 = 12\cdot 11\cdot 10\cdot 6 = 11\cdot 10\cdot 9\cdot 8$$

or

$$\text{(II)}\quad 22\times(A_5:1) = 22\cdot5\cdot4\cdot3=12\cdot11\cdot10.$$

Now we show that G is triply transitive. As it is doubly transitive it suffices to show that

$$(4)\qquad X^{10} + (\alpha+\beta)X^9 + (\alpha^2+\alpha\beta+\beta^2)X^8 +\cdots+ (\alpha^{10}+\alpha^9\beta+\cdots+\alpha^{10})$$

is irreducible over $k(\alpha, \beta)$, where α and β are two roots of $X^{12}-aX+b=0$. We assume it is reducible. As

$$X^{10} + X^9 +\cdots+ X + 1$$

is factorized to two irreducible factors of degree 5 over k, (4) is also a product

$$g(\alpha, \beta, X)h(\alpha, \beta, X)$$

of factors of degree 5. As (4) is symmetric for α and β,

$$g(\beta, \alpha, X) = g(\alpha, \beta, X)$$

or

$$g(\beta, \alpha, X) = h(\alpha, \beta, X)$$

holds. If the latter is true, (4) must be a square when we put $\alpha=\beta$. But this is not the case. In the former case, its constant term is a symmetric form of α and β of degree 5. Then it is a multiple of $\alpha+\beta$. But $\alpha+\beta$ is not a factor of $\alpha^{10}+\alpha^9\beta+\cdots+\beta^{10}$. This is a contradiction. Therefore (4) must be irreducible. In the case (II), $k(\alpha, \beta, \gamma)$ must be equal to K for any root γ of (4). If we put $\alpha=\beta$ in (4), we have

$$\begin{aligned}&X^{10} - \alpha X^9 + \alpha^3X^7 - \alpha^4X^6 + \alpha^6X^4 - \alpha^7X^3 + \alpha^9X - \alpha^{10}\\ &= (X-\alpha)(X+\alpha)^3(X^2+\alpha^2)^3\,.\end{aligned}$$

Then (4) has a factor of degree 1 and a factor of degree greater that 1 in the complete field $k(\alpha)(\beta)_{\beta-\alpha}$. So the case (II) does not hold. Therefore we have

$$(G:1) = 12\cdot11\cdot10\cdot6 = 11\cdot10\cdot9\cdot8\,;$$

Let α be a root of $X^{12}-aX+b=0$, and let G_α be a subgroup of G fixing α. As G is triply transitive, G_α is doubly transitive of order $11\cdot 10\cdot 6$. Then it is not solvable, and by considering its order it must be a simple group. Then G is also a simple group by [3. Proposition 4. 5]. As c^2 satisfies an irreducible equation

$$X^{11}+b^3X^2-a^4=0\,,$$

and as G is simple, the splitting field of this equation is K. Namely G is represented as a permutation group of degree 11. Then it must be isomorphic to Mathieu group M_{11} by [1]. Above argument and [1] also shows that the Galois group of $X^{11}+aX^2+b=0$ is isomorphic to M_{11}.

REFERENCES

[1] F. N. COLE, List of the transitive substitution groups of ten and of eleven letters, Quart. J. Math., 27(1895).

[2] B. HUPPERT, Zweifach transitive auflösbare Permutations-gruppen, Math. Z., 68(1957).

[3] D. S. PASSMAN, Permutation groups, Benjamin, 1968.

[4] K. UCHIDA, Unramified extensions of quadratic number fields II, Tôhoku Math. J., 22 (1970).

[5] H. WIELANDT, Finite permutation groups, Academic Press, 1964.

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, JAPAN.