35. *Galois Groups of Polynomials*

By Mitsuo YOSHIZAWA
College of General Education, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1984)

1. Let $f(x) \in K[x]$ be a monic irreducible polynomial of degree n over a field K of characteristic 0. Several theoretical algorithms for the determination of the Galois group $\mathrm{Gal}_K(f)$ of $f(x)$ over K have been developed by many authors (cf. van der Waerden [5], Zassenhaus [7], Stauduhar [4]), but it is known that the practical determination is difficult for large n. In [1] a technique for determining the set-transitivity of the Galois group of a polynomial is described by Erbach, Fischer and Mckay, and they prove that $x^7-154x+99$ has the Galois group $PSL(2,7)$. In [3] Jensen and Yui give a criterion characterizing $f(x)$ with $\mathrm{Gal}_K(f)\cong D_p$ (the dihedral group of prime degree p).

In this paper we give criteria characterizing $f(x)$ which has as $\mathrm{Gal}_K(f)$ a group with some properties as a permutation group. In particular, we give a formula giving the order of $\mathrm{Gal}_K(f)$.

2. We state several terminologies [6] concerning the permutation group theory. Let G be a permutation group on Ω. We say that a subset Δ of Ω is an *orbit* of G if $(\Delta)G=\Delta$ and G acts transitively on Δ. G is called *t-transitive* on Ω if for every two ordered t-tuples $\alpha_1, \cdots, \alpha_t$ and $\beta_1, \cdots, \beta_t$ of elements of Ω (with $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$ for $i \neq j$) there exists $g \in G$ with $(\alpha_i)g=\beta_i$ $(i=1, \cdots, t)$. If G is transitive on Ω and if there is a subset Γ $(1<|\Gamma|<|\Omega|)$ of Ω satisfying $(\Gamma)g=\Gamma$ or $(\Gamma)g \cap \Gamma=\phi$ for all $g \in G$, G is called an *imprimitive group* on Ω with a *block* Γ. (Then $|\Gamma|\,|\,|\Omega|$ holds obviously.) We say G is *primitive* on Ω if G is transitive but not imprimitive on Ω. Obviously G is primitive if G is doubly transitive. For s elements $\alpha_1, \cdots, \alpha_s \in \Omega$ we set $G_{\alpha_1\cdots\alpha_s}=\{g \in G : (\alpha_i)g=\alpha_i,\ i=1, \cdots, s\}$, a subgroup of G.

3. From now on, we assume $G=\mathrm{Gal}_K(f)$ and $\Omega=$ the set of roots of $f(x)$. For independent variables $X_1, \cdots, X_n$

$$\prod_{(\alpha_1,\cdots,\alpha_n)\neq(\alpha_1',\cdots,\alpha_n')\in\Omega\times\cdots\times\Omega}\{(\alpha_1-\alpha_1')X_1+(\alpha_2-\alpha_2')X_2+\cdots+(\alpha_n-\alpha_n')X_n\}$$

is a non-zero polynomial in $K[X_1, \cdots, X_n]$ of degree $n^n(n^n-1)$. Hence there exist distinct non-zero rational integers $a_1, \cdots, a_n$ with

$$\prod_{(\alpha_1,\cdots,\alpha_n)\neq(\alpha_1',\cdots,\alpha_n')\in\Omega\times\cdots\times\Omega}\{a_1(\alpha_1-\alpha_1')+a_2(\alpha_2-\alpha_2')+\cdots+a_n(\alpha_n-\alpha_n')\}\neq 0.$$

Hereafter we fix $a_1, a_2, \cdots, a_n$. For each m $(1\leqq m\leqq n)$ we define

$$\Phi_{(a_1,a_2,\cdots,a_m)}(X)=\prod_{(\alpha_1,\cdots,\alpha_m)\in\Omega\times\cdots\times\Omega}(X-(a_1\alpha_1+a_2\alpha_2+\cdots+a_m\alpha_m)).$$

Then it is a polynomial in $K[X]$ of degree n^m of which all roots are distinct from one another.

Now there exist a natural number s and mappings Δ_i $(i=0,1,\cdots,s)$ from Ω into the subsets of Ω, such that Ω decomposes into exactly $(s+1)$ G_α-orbits $\Delta_0(\alpha)=\{\alpha\}$, $\Delta_1(\alpha),\cdots,\Delta_s(\alpha)$ for each $\alpha\in\Omega$ satisfying $(\Delta_i(\alpha))g=\Delta_i((\alpha)g)$ for all $\alpha\in\Omega$, $g\in G$, $i=0,1,\cdots,s$. We call Δ_i $(0\leqq i\leqq s)$ an *orbital* [2] of G. The number $|\Delta_i(\alpha)|$, which is independent of $\alpha\in\Omega$, is called the *length* $|\Delta_i|$ of Δ_i. Then we have

Theorem 1. *$\Phi_{(a_1,a_2)}(X)=f_0(X)f_1(X)\cdots f_s(X)$ holds, where*

$$f_i(X)=\prod_{\alpha\in\Omega}\prod_{\beta\in\Delta_i(\alpha)}(X-(a_1\alpha+a_2\beta))\qquad(0\leqq i\leqq s)$$

is an irreducible polynomial in $K[X]$ with $\deg f_i/n=|\Delta_i|$ $(i=0,\cdots,s)$.

4. Let Δ_i be an arbitrarily fixed orbital with $i\geqq 1$. Then there exist a natural number r and mappings $\Gamma_j=\Gamma_j^{(\Delta_i)}$ $(j=0,1,\cdots,r)$ from $T=\{(\alpha,\beta):\alpha\in\Omega,\ \beta\in\Delta_i(\alpha)\}$ into the subsets of Ω, such that Ω decomposes into exactly $(r+1)$ $G_{\alpha\beta}$-orbits

$$\Gamma_0(\alpha,\beta)=\{\alpha\},\quad\Gamma_1(\alpha,\beta)=\{\beta\},\quad\Gamma_2(\alpha,\beta),\cdots,\Gamma_r(\alpha,\beta)$$

for each $(\alpha,\beta)\in T$ satisfying $(\Gamma_j(\alpha,\beta))g=\Gamma_j((\alpha)g,(\beta)g)$ for all $(\alpha,\beta)\in T$, $g\in G$, $j=0,1,\cdots,r$. The number $|\Gamma_j(\alpha,\beta)|$, which is independent of $\alpha\in\Omega$ and $\beta\in\Delta_i(\alpha)$, is called the *length* $|\Gamma_j^{(\Delta_i)}|$ of $\Gamma_j^{(\Delta_i)}$.

For $f_i(X)$ (corresponding to Δ_i) we define

$$\Phi^{(f_i)}_{(a_1,a_2,a_3)}(X)=\prod_{\gamma\in\Omega}f_i(X-a_3\gamma).$$

Then it is a divisor of $\Phi_{(a_1,a_2,a_3)}(X)$ in $K[X]$, and we get

Theorem 2. *$\Phi^{(f_i)}_{(a_1,a_2,a_3)}(X)=h_0(X)h_1(X)\cdots h_r(X)$ holds, where*

$$h_j(X)=\prod_{\alpha\in\Omega}\prod_{\beta\in\Delta_i(\alpha)}\prod_{\gamma\in\Gamma_j(\alpha,\beta)}(X-(a_1\alpha+a_2\beta+a_3\gamma))\qquad(0\leqq j\leqq r)$$

is an irreducible polynomial in $K[X]$ with $\deg h_j/(n|\Delta_i|)=|\Gamma_j^{(\Delta_i)}|$ $(j=0,1,\cdots,r)$.

Remark. In Theorems 1 and 2, $s=1$ holds if and only if G is doubly transitive on Ω, and moreover $r=2$ holds if and only if G is triply transitive on Ω.

5. We can continue arguments of Theorems 1, 2, $\cdots$ similarly. Hence by this method we can get $|G|$ essentially because of the following lemma (cf. [6, Theorem 3.2, Proposition 3.3]).

Lemma. *If $G_{\gamma_1\cdots\gamma_v}=\{1\}$ holds for v elements $\gamma_1,\cdots,\gamma_v$ in Ω, we have $|G|=|(\gamma_1)G||(\gamma_2)G_{\gamma_1}|\cdots|(\gamma_v)G_{\gamma_1\cdots\gamma_{v-1}}|$ where $|(\gamma_k)G_{\gamma_1\cdots\gamma_{k-1}}|$ is the length of the orbit of $G_{\gamma_1\cdots\gamma_{k-1}}$ containing γ_k.*

6. Let us suppose that n is not prime and d is a divisor of n with $1<d<n$. Assuming that $\varphi_i(X_1,\cdots,X_d)$ $(i=1,\cdots,d)$ are the elementary symmetric polynomials of $X_1,\cdots,X_d$ and that $\Omega^{(d)}$ is the set of d-element subsets of Ω, then for independent variables $Y_1,\cdots,Y_d$

$$\prod_{\{\alpha_1,\cdots,\alpha_d\}\neq\{\alpha_1',\cdots,\alpha_d'\}\in\Omega^{(d)}}\left\{\sum_{i=1}^{d}Y_i(\varphi_i(\alpha_1,\cdots,\alpha_d)-\varphi_i(\alpha_1',\cdots,\alpha_d'))\right\}$$

is a non-zero polynomial in $K[Y_1, \cdots, Y_d]$ of degree $\binom{n}{d}\left(\binom{n}{d}-1\right)$. Hence there exist rational integers $b_1, \cdots, b_d$ with

$$\prod_{\{\alpha_1,\cdots,\alpha_d\}\neq\{\alpha'_1,\cdots,\alpha'_d\}\in\Omega^{(d)}} \left\{\sum_{i=1}^{d} b_i(\varphi_i(\alpha_1, \cdots, \alpha_d)-\varphi_i(\alpha'_1, \cdots, \alpha'_d))\right\}\neq 0.$$

Hereafter we fix $b_1, \cdots, b_d$. If we define

$$\Psi_{(b_1,\cdots,b_d)}(X)=\prod_{\{\alpha_1,\cdots,\alpha_d\}\in\Omega^{(d)}} \{X-(b_1\varphi_1(\alpha_1, \cdots, \alpha_d)+\cdots+b_d\varphi_d(\alpha_1, \cdots, \alpha_d))\},$$

then it is a polynomial in $K[X]$ of degree $\binom{n}{d}$ of which all roots are distinct from one another, and we get

Theorem 3. *$\Psi_{(b_1,\cdots,b_d)}(X)$ has an irreducible factor of degree n/d in $K[X]$ if and only if G is an imprimitive group whose block-size is d.*

In Theorem 3 if $\lambda(X)$ is an irreducible factor of $\Psi_{(b_1,\cdots,b_d)}(X)$ of degree n/d, then we may assume that G has n/d blocks $\Delta_i=\{\alpha_{i1}, \cdots, \alpha_{id}\}$ $(i=1, \cdots, n/d)$ with $\Omega=\Delta_1+\cdots+\Delta_{n/d}$ satisfying

$$\lambda(X)=\prod_{i=1}^{n/d} \{X-(b_1\varphi_1(\alpha_{i1}, \cdots, \alpha_{id})+\cdots+b_d\varphi_d(\alpha_{i1}, \cdots, \alpha_{id}))\}.$$

Let $\bar{G}$ be the permutation group on $\bar{\Omega}=\{\Delta_1, \cdots, \Delta_{n/d}\}$ induced by G. Then we have

Theorem 4. $\bar{G}\cong\mathrm{Gal}_K(\lambda)$.

References

[1] D. W. Erbach, J. Fischer, and J. Mckay: Polynomials with PSL(2,7) as Galois group. J. Number Theory, **11**, 69–75 (1979).

[2] D. G. Higman: Intersection matrices for finite permutation groups. J. Algebra, **6**, 22–42 (1967).

[3] C. U. Jensen and N. Yui: Polynomials with D_p as a Galois group. J. Number Theory, **15**, 347–374 (1982).

[4] R. P. Stauduhar: The determination of Galois groups. Math. Comput., **27**, 981–996 (1973).

[5] B. van der Waerden: Modern Algebra. vol. 1, Unger, New York (1953).

[6] H. Wielandt: Finite Permutation Groups. Academic Press, New York-London (1964).

[7] H. Zassenhaus: On the group of an equation. Nachr. Akad. Gött. Math.-Phys., Kl.II, 147–166 (1967).