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

$$\prod_{(\alpha_1,\cdots,\alpha_n)\neq(\alpha'_1,\cdots,\alpha'_n)\in\Omega\times\cdots\times\Omega}\{a_1(\alpha_1-\alpha'_1)+a_2(\alpha_2-\alpha'_2)+\cdots+a_n(\alpha_n-\alpha'_n)\}\neq0.$$

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

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