PACIFIC JOURNAL OF MATHEMATICS
Vol. 163, No. 1, 1994

# NONRIGID CONSTRUCTIONS IN GALOIS THEORY

PIERRE DEBES AND MICHAEL D. FRIED

**The context for this paper is the *Inverse Galois Problem*. First we give an if and only if condition that a finite group is the group of a Galois regular extension of $\mathbb{R}(X)$ with only real branch points. It is that the group is generated by elements of order 2 (Theorem 1.1 (a)). We use previous work on the action of the complex conjugation on covers of $\mathbb{P}^1$. We also show each finite group is the Galois group of a Galois regular extension of $\mathbb{Q}^{tr}(X)$. Here $\mathbb{Q}^{tr}$ is the field of all totally real algebraic numbers (Theorem 5.7). Sections 1, 2, and 3 discuss consequences, generalizations, and related questions.**

**The second part of the paper, §4 and §5, concerns descent of fields of definition from $\mathbb{R}$ to $\mathbb{Q}$. Use of Hurwitz families reduces the problem to finding $\mathbb{Q}$-rational point on a special algebraic variety. Our first application considers realizing the symmetric group $S_m$ as the group of a Galois extension of $\mathbb{Q}(X)$, regular over $\mathbb{Q}$, satisfying two further conditions. These are that the extension has four branch points, and it also has some totally real residue class field specializations. Such extensions exist for $m = 4, 5, 6, 7, 10$ (Theorem 4.11).**

**Suppose that $m$ is a prime larger than 7. Theorem 5.1 shows that the dihedral group $D_m$ of order $2m$ is not the group of a Galois regular extension of $\mathbb{Q}(X)$ with fewer than 6 branch points. The proof interprets realization of certain dihedral group covers as corresponding to rational points on *modular curves*. We then apply Mazur's Theorem. New results of Kamienny and Mazur suggest that no bound on the number of branch points will allow realization of all $D_m$ s.**

**0.1. Description of Theorem 1.1.** Throughout, $\mathbb{C}$ denotes the complex number field, $X$ an indeterminate, and $\overline{\mathbb{C}(X)}$ a fixed algebraic closure of $\mathbb{C}(X)$. Let $k$ be a subfield of $\mathbb{C}$. We say a finite extension $Y/k(X)$ with $\overline{\mathbb{C}(X)} \supset Y$ is regular over $k$ if $\overline{k} \cap Y = k$. Equivalently $[Y\colon k(X)] = [Y\mathbb{C}\colon \mathbb{C}(X)]$. Denote this degree by $n$. Regard the degree $n$ field extension $Y\mathbb{C}/\mathbb{C}(X)$ as the function field extension of a degree $n$ cover $\varphi\colon Y_{\mathbb{C}} \to \mathbb{P}^1$. Here $\mathbb{P}^1$ is the complex projective line and $Y_{\mathbb{C}}$ is an irreducible non-singular curve.

The map $\varphi$ is ramified over a finite number of points $x_1, \ldots, x_r$. We call these the *branch points* of the cover (or of the extension $Y/k(X)$). Our first result (Theorem 1.1(a)) shows exactly when a finite group $G$ is the group of a Galois regular extension of $\mathbb{R}(X)$ with only real branch points.