ELLIPTIC CURVES AND ALTERNATING GROUP EXTENSIONS OF THE RATIONAL NUMBERS

(Order No.   )

MARK FRASER EVANS

Boston University Graduate School of Arts and Sciences, 2001

Major Professor: David E. Rohrlich, Professor of Mathematics

ABSTRACT

The inverse Galois problem asks if each finite group G is the Galois group of some extension of the rational numbers $\mathbb{Q}$. The modern approach to this problem involves exhibiting a regular G-Galois cover of curves $C \longrightarrow \mathbb{P}_1$ defined over $\mathbb{Q}$. The corresponding extension of function fields $\mathbb{Q}(C)/\mathbb{Q}(\mathbb{P}_1)$ is then Galois with group G. One uses Hilbert's irreducibility theorem to conclude that there exist infinitely many rational points in $\mathbb{P}_1(\mathbb{Q})$ which "specialize" to give a Galois extension of $\mathbb{Q}$ with group G.

In this thesis, we consider the case where $\mathbb{P}_1$ is replaced by an elliptic curve $E/\mathbb{Q}$ with positive Mordell-Weil rank. A theorem of Néron and Serre says that if a group G is perfect then a regular G-Galois cover $C \longrightarrow E$ defined over $\mathbb{Q}$ can be specialized to *almost any* point in $E(\mathbb{Q})$ to obtain a Galois extension of $\mathbb{Q}$ with group G. We use this theorem to realize the alternating groups A_n ($n \not\equiv 3 \bmod 6$) as Galois groups over $\mathbb{Q}$. This is the first time an infinite family of groups has

been realized using this variant of the classical Hilbert irreducibility theorem.