BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 24, Number 1, January 1991

$PSL_2(q)$ AND EXTENSIONS OF $\mathbf{Q}(x)$

HELMUT VÖLKLEIN

INTRODUCTION

We recall that an extension $K/\mathbf{Q}(x)$ of finite degree n is called *regular* if $\mathbf{Q}$ is algebraically closed in K. Tensoring with the complex field $\mathbf{C}$ we obtain the extension $\overline{K}/\mathbf{C}(x)$ of degree n. Since $\mathbf{C}(x)$ is the function field of the Riemann sphere $\mathbf{P}^1$, the field extension $\overline{K}/\mathbf{C}(x)$ corresponds to a cover $X \to \mathbf{P}^1$ of Riemann surfaces. All but finitely many points of $\mathbf{P}^1$ have exactly n preimages in X, and these finitely many exceptional points are called the *branch points.*

If a finite group G is the Galois group of a regular extension of $\mathbf{Q}(x)$, then G occurs as a Galois group over every number field (by Hilbert's irreducibility theorem). This is the basis of all recent work on the inverse problem of Galois theory (by Fried, Matzat, Thompson, and others). An important invariant of a regular extension of $\mathbf{Q}(x)$ is the number r of branch points. Most work has been concentrated on the case $r = 3$, using Thompson's concept of rigidity [Th1]. Indeed, the case $r = 3$ seems at first the natural one to work with, since it involves using $r - 1 = 2$ generators of the group under consideration, and it is known that every (finite) simple group can be generated by two elements; furthermore, the rigidity condition becomes too stringent for $r > 3$, and there seems only one example known (due to Thompson) of a simple group for which rigidity holds with $r > 3$.

It appears that for $r > 3$ one has to include the action of the Hurwitz monodromy group (see §2), which goes back to [Fr1]. Indeed Matzat [Ma1, Chapter III] has used this action to realize a few groups as Galois groups over $\mathbf{Q}(x)$ with $r > 3$. However, by far the most simple groups (and related groups) that are known so far to be Galois groups over $\mathbf{Q}$ (or over certain number fields) have

Received by the editors January 23, 1990 and, in revised form, April 28, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G35, 12F10, 14E20, 14G05, 20B25, 20C25.
Partially supported by NSA grand MDA 904-89-H-2028.

0273-0979/91 $1.00 + $.25 per page

been realized with $r = 3$: e.g., over $\mathbf{Q}$, the monster group [Th1] and several other sporadic simple groups ([Ma2, HS, Hunt, etc.]), the groups $\mathrm{PSL}_2(p)$ for primes $p \not\equiv \pm 1 \pmod{24}$ [Sh, MM], the groups $\mathrm{PSL}_3(p)$ for primes $p \equiv 1 \pmod 4$ [Th2], the orthogonal groups $O^-_{\ell-1}(2)$ for primes $\ell \geq 11$ with 2 as a primitive root mod ℓ [Th3]), the exceptional Chevalley groups $G_2(p)$ for primes $p \geq 5$ ([Th4, FF]), the groups $\mathrm{PSL}_2(p^2)$ for primes $p \equiv \pm 2 \pmod 5$ [F1], certain special unitary groups $\mathrm{SU}_3(p)$ [Malle2], certain groups $E_8(p)$ [Malle1].

In particular, we see that the Chevalley groups that have been realized over $\mathbf{Q}$ comprise only groups over fields of prime order p, or order p^2. Here we show that indeed *not* all simple groups can be realized with three branch points:

Theorem. *Let p be any prime. If $n > 8$ then the group $\mathrm{PSL}_2(p^n)$ does not occur as Galois group of a regular extension of $\mathbf{Q}(x)$ with three branch points.*

This indicates the need to consider the case of $r \geq 4$ branch points, as in [FrTh; Fr2; Ma1, Kap. III; FrVo]. It was brought to my attention that J. Thompson has obtained similar results as in the above theorem (unpublished) for $\mathrm{PSL}_2(3^n)$.

The proof of the theorem will be indicated in §3. In §2, we discuss how the groups $\mathrm{PSL}_2(q)$ relate to the approach via Hurwitz spaces and Nielsen classes, due to M. Fried [Fr1] and developed further in [FrVo].

2. Hurwitz spaces and $\mathrm{PSL}_2(q)$

The general results described in §2.1 are contained in [Fr1, Fr2, FrVo].

2.1. **The General Set-up.** Let G be a finite group and let $\mathscr{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G. Let N be the least common multiple of the orders of the elements in these conjugacy classes. We assume that for each integer m prime to N and for each $(\sigma_1, \ldots, \sigma_r) \in C_1 \times \cdots \times C_r$ we have $(\sigma_1^m, \ldots, \sigma_r^m) \in C_{\pi(1)} \times \cdots \times C_{\pi(r)}$ for some $\pi \in S_r$. (This generalizes the usual notion of a rational conjugacy class, so we say $\mathscr{C}$ is a *rational* r-tuple of conjugacy classes).

Let $\mathrm{Ni}(\mathscr{C})$ be the set of all $(\sigma_1, \ldots, \sigma_r) \in G^r$ with $< \sigma_1, \ldots, \sigma_r >= G$ and $\sigma_1 \ldots \sigma_r = 1$, such that $(\sigma_1, \ldots, \sigma_r) \in C_{\pi(1)} \times \cdots \times C_{\pi(r)}$ for some $\pi \in S_r$. Let A denote the group of inner

automorphisms of G (resp., the group of those automorphisms of G that permute the conjugacy classes $C_1, \ldots, C_r$). Then we define the set N^{in} of *inner Nielson classes* (resp., the set N^{ab} of *absolute Nielsen classes*) to be the quotient of $\text{Ni}(\mathscr{C})$ by the (componentwise) action of A.

Let $\mathbf{P}^1$ be the Riemann sphere, and let $\mathscr{U}^{(r)}$ be the space of r-tuples $(x_1, \ldots, x_r)$ of pairwise distinct points from $\mathbf{P}^1$. Further, $\mathscr{U}_r$ denotes the quotient of $\mathscr{U}^{(r)}$ by the natural action of S_r (permuting $x_1, \ldots, x_r$). View $\mathscr{U}_r$ as the space of all unordered r-tuples of distinct points from $\mathbf{P}^1$. The fundamental group of $\mathscr{U}_r$ is the *Hurwitz monodromy group* H_r. It has generators $Q_1, \ldots, Q_{r-1}$ (the "simple braidings"), which define a permutation action of H_r on N^{in} and on N^{ab} by the following rule:

Q_i sends the class of $(\sigma_1, \ldots, \sigma_r)$

to the class of $(\sigma_1, \ldots, \sigma_i\sigma_{i+1}\sigma_i^{-1}, \sigma_i, \ldots, \sigma_r)$.

These permutation representations of the fundamental group of $\mathscr{U}_r$ define covering spaces $\mathscr{H}^{\text{in}}$ (resp. $\mathscr{H}^{\text{ab}}$) of $\mathscr{U}_r$, fitting in the sequence

$$\mathscr{H}^{\text{in}} \xrightarrow{\Phi} \mathscr{H}^{\text{ab}} \xrightarrow{\Psi} \mathscr{U}_r.$$

By the theory of covering spaces, the connected components of $\mathscr{H}^{\text{ab}}$ and $\mathscr{H}^{\text{in}}$ correspond to the orbits of H_r on N^{ab} and on N^{in}, respectively.

The space $\mathscr{H}^{\text{ab}}$ is a moduli space for Galois covers (of Riemann surfaces) $f: X \to \mathbf{P}^1$ with monodromy group G and with the property that some description of branch cycles of f lies in $\text{Ni}(\mathscr{C})$. That is, each point $\mathbf{p} \in \mathscr{H}^{\text{ab}}$ corresponds to exactly one equivalence class of such covers f, and thereby $\Psi(\mathbf{p})$ is the unordered tuple of branch points of f (see [Fr2, §3.3]).

For technical reasons we now assume G has a self-normalizing subgroup H containing no normal subgroup $\neq 1$ of G, such that the conjugacy class of H is invariant under $\text{Aut}(G)$. (This is true for all simple groups G.) When this holds we are able to assert a key property of the space $\mathscr{H}^{\text{in}}$. The Galois group $\Gamma = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ permutes the connected components of the spaces $\mathscr{H}^{\text{ab}}$ and $\mathscr{H}^{\text{in}}$, and if such a component is fixed by Γ then it can be viewed naturally as an algebraic variety defined over $\mathbf{Q}$. Now let $\mathbf{p}_0$ be a point on such a Γ-fixed component $\mathscr{H}$ of $\mathscr{H}^{\text{in}}$. If $\mathbf{p} = \Phi(\mathbf{p}_0)$ is a $\mathbf{Q}$-rational point of $\Phi(\mathscr{H})$ then each cover $f: X \to \mathbf{P}^1$

corresponding to $\mathbf{p}$ can be defined over $\mathbf{Q}$, and if $\mathbf{p}_0$ is already a $\mathbf{Q}$-rational point then $\mathbf{Q}(X)$ is Galois over $\mathbf{Q}(\mathbf{P}^1) = \mathbf{Q}(x)$; in the latter case, $\mathbf{Q}(X)/\mathbf{Q}(x)$ is a regular Galois extension with Galois group G (and r branch points).

2.2. **Examples for** $r = 3$. Let $G = \mathrm{PSL}_2(p)$ for a prime $p > 3$. If G has elements of order $m \leq 4$, then these elements form a single conjugacy class $\bar{m}$.

Example 1. Suppose $p \equiv \pm 1 \pmod 8$, and $\mathscr{C} = (\bar{4}, \bar{4}, \bar{4})$. Then $\mathrm{SL}_2(p)$ has two conjugacy classes C, C' of elements of order 8, and $\mathrm{Ni}(\mathscr{C})$ is the disjoint union of the image of $\mathrm{Ni}(C, C, C)$ and of the image of $\mathrm{Ni}(C', C', C')$. Thus, by Lemma 2, N^{ab} consists of two elements, both of which are fixed by the Hurwitz group H_3. This means that the space $\mathscr{H}^{\mathrm{ab}}$ consists of two components. It follows from the "branch cycle argument" of [Fr1, p. 63] that these components are interchanged by Γ. Therefore none of the covers f parametrized by $\mathscr{H}^{\mathrm{ab}}$ can be defined over $\mathbf{Q}$.

Example 2. Suppose again $p \equiv \pm 1 \pmod 8$, and $\mathscr{C} = (\bar{4}, \bar{4}, \bar{3})$. Then the triples $(\sigma_1, \sigma_2, \sigma_3) \in \bar{4} \times \bar{4} \times \bar{3}$ with $\sigma_1\sigma_2\sigma_3 = 1$ fall into two classes under $\mathrm{PGL}_2(p)$, with the triples in one class generating G and the triples in the other class generating a subgroup isomorphic S_4 (cf. [Malle3, 6.2]). Thus only the first kind of triples appear in $\mathrm{Ni}(\mathscr{C})$, and N^{ab} consists of three elements, which are permuted transitively by the Hurwitz group H_3. Hence $\mathscr{H}^{\mathrm{ab}}$ is irreducible, and can be identified as $\mathscr{U}^{(3)}/\langle(12)\rangle$. It follows that all the covers f parametrized by $\mathscr{H}^{\mathrm{ab}}$ and having rational branch points can be defined over $\mathbf{Q}$. Furthermore, the space $\mathscr{H}^{\mathrm{in}}$ is irreducible if and only if $p \equiv \pm 7 \pmod{24}$; in this case, $\mathscr{H}^{\mathrm{in}} \cong \mathscr{U}^{(3)}$ has lots of $\mathbf{Q}$-rational points, and we have realized G as the Galois group of a regular extension of $\mathbf{Q}(x)$ with ramification structure $(\bar{4}, \bar{4}, \bar{3})$. This was done by a different method in [MM, Satz 2] and in [Malle3, 6.4]. If $p \equiv \pm 1 \pmod{24}$, then $\mathscr{H}^{\mathrm{in}}$ has two components, and it is not clear whether they are interchanged by Γ or not. If not, then we have again realized G as Galois group of a regular extension of $\mathbf{Q}(x)$ with three branch points. This is interesting because if $p \equiv \pm 1 \pmod{24}$ and 7 is a quadratic residue mod p, then it is not known so far whether G occurs *at all* as a Galois group over $\mathbf{Q}$ (cf. [Sh, MM]).

2.3. **Increasing the number of branch points.** Consider again $G = \mathrm{PSL}_2(q)$. For $r = 3$ the problem is that $\mathrm{Ni}(\mathscr{C})$ may be empty (as

in §3 below) or $\mathscr{H}^{\text{in}}$ may not be connected (as in §2.2). Both of these difficulties disappear for larger r: Firstly, it follows from a theorem of Conway and Parker [CP] that if $\mathscr{C}$ contains the conjugacy class of involutions a suitably large number of times then $\mathscr{H}^{\text{in}}$ will be connected. Secondly, the cardinality of N^{in} grows very fast with r, it will roughly be of the order of magnitude $q^{2(r-3)}$. Unfortunately, the latter fact creates new difficulties: When $\mathscr{H}^{\text{in}}$ is a high degree cover of $\mathscr{U}_r$ then it becomes very difficult to study this variety, and in particular to find a rational point on it.

3. The proof of the main theorem

We give a proof of the theorem stated in the Introduction in the case $n > 12$:

By [Fr1, Corollary 5.2] we know that if a finite group G occurs as Galois group of a regular (Galois) extension of $\mathbf{Q}(x)$ with three branch points, then G has generators $\sigma_1, \sigma_2, \sigma_3$ with $\sigma_1\sigma_2\sigma_3 = 1$ that satisfy:

(1) For any integer k prime to the order of each σ_i there is a permutation $\pi \in S_3$ such that σ_i^k is conjugate to $\sigma_{\pi(i)}$ for $i = 1, 2, 3$.

Now let p be a prime, and $G = \text{PSL}_2(q)$, $q = p^n$. Let $\sigma_1, \sigma_2, \sigma_3$ be generators of G with $\sigma_1\sigma_2\sigma_3 = 1$, satisfying (1). We will show that this forces $n \leq 12$.

We need the following elementary properties of the group $G = \text{PSL}_2(q)$ (see e.g., [Hu, Kap. II,8]): Each $g \in G$ is either of order p or of order prime to p; in particular, g is a p-element or a p'-element. Furthermore, for any integer k we have:

If $g \in G$ is a p'-element, then g is conjugate to g^k if and only if $g^k = g^{\pm 1}$.

If g is a p-element, then g is conjugate to g^k if and only if k is a (nonzero) square mod p.

Let $\varphi(\sigma_i)$ denote the number of generators of the cyclic group $\langle\sigma_i\rangle$. The following is an easy consequence of (1):

Lemma 1. (a) *Suppose $p \neq 2$. Then either none or two of the σ_i's are p-elements. If, say, σ_2 and σ_3 are p-elements, then $\varphi(\sigma_1) \leq 2$.*

(b) *Suppose that either $p = 2$ or none of $\sigma_1, \sigma_2, \sigma_3$ is a p-element. Then either $\{\varphi(\sigma_1), \varphi(\sigma_2), \varphi(\sigma_3)\} \subset \{1, 2, 4\}$ or $\varphi(\sigma_1) = \varphi(\sigma_2) = \varphi(\sigma_3) = 6$.*

Now choose elements $\tau_1, \tau_2, \tau_3 \in \mathrm{SL}_2(q)$ mapping to $\sigma_1, \sigma_2, \sigma_3$, respectively. Then these elements generate $\mathrm{SL}_2(q)$. Since $\sigma_1\sigma_2\sigma_3 = 1$, we can arrange it that $\tau_1\tau_2\tau_3 = 1$. Set $t_i = \mathrm{tr}(\tau_i)$ for $i = 1, 2, 3$. If $t_1 = \pm 2$ then σ_1 is a p-element. Thus, by Lemma 1(a), we may assume with no loss that $t_1 \neq \pm 2$. (Note that for $p = 2$ each p-element is an involution.) Let K be the subfield of $\mathbf{F}_q$ generated by t_1, t_2, t_3. Then $K = \mathbf{F}_q$ by Lemma 2 below. Thus from the following assertion we get $n \leq 12$, as desired.

$$[K: \mathbf{F}_p] \leq 12. \tag{2}$$

To prove (2), note that $\varphi(\tau_i) = \varphi(\sigma_i)$ or $\varphi(\tau_i) = 2\varphi(\sigma_i)$. Let I be the set of those $i = 1, 2, 3$ for which σ_i is a p'-element. From Lemma 1 it follows that either all of the $\varphi(\tau_i)$, $i \in I$, divide 8, or all of them divide 12.

Clearly, K is contained in the field generated by the eigenvalues of the τ_i, $i \in I$. The eigenvalues ζ_i, ζ_i^{-1} of such a τ_i are primitive e_i-th roots of unity, where e_i is the order of τ_i. Thus the degree $[\mathbf{F}_p(\zeta_i): \mathbf{F}_p]$ is a divisor of $\varphi(\tau_i)$. Now it follows from the last paragraph that either all the ζ_i, $i \in I$, lie in $\mathbf{F}_{p^8}$, or they all lie in $\mathbf{F}_{p^{12}}$. Thus $K \subset \mathbf{F}_{p^8}$ or $K \subset \mathbf{F}_{p^{12}}$. This proves (2).

Remark 1. The case $\varphi(\tau_1) = \varphi(\tau_2) = \varphi(\tau_3) = 12$ is not excluded by condition (1), but it actually cannot arise from a realization of G as Galois group of a regular extension of $\mathbf{Q}(x)$ with three branch points. This can be seen as in Example 1. Once this case is excluded, the above shows that $n \leq 8$, completing the proof of the theorem.

Remark 2. For $p = 2$ we get more precisely that $\mathrm{PSL}_2(2^n)$ occurs as Galois group of a regular extension of $\mathbf{Q}(x)$ with three branch points if and only if $n \leq 3$. (The "if-part" is well known, see [Ma1] for example).

Lemma 2. *Let t_1, t_2, t_3 be elements of the field $\mathbf{F}_q$, $q = p^n$, and suppose $t_1 \neq \pm 2$. Then the following hold:*

(a) *All triples (τ_1, τ_2, τ_3) of elements of $\mathrm{SL}_2(q)$ with the following properties are conjugate under $\mathrm{GL}_2(q)$: $\tau_1\tau_2\tau_3 = 1$, τ_1, τ_2, τ_3 do not have a common eigenvector, and $\mathrm{tr}(\tau_i) = t_i$ $(i = 1, 2, 3)$.*

(b) *If any such triple (τ_1, τ_2, τ_3) as in* (a) *generates $\mathrm{SL}_2(q)$, then the traces t_1, t_2, t_3 generate the field $\mathbf{F}_q$.*

Proof of (a). Let (τ_1, τ_2, τ_3) be a triple with the above properties. The eigenvalues ζ, ζ^{-1} of τ_1 are determined by t_1, and they are distinct since $t_1 \neq \pm 2$. If $\zeta \notin \mathbf{F}_q$ we embed $\mathrm{GL}_2(q)$ into $\mathrm{GL}_2(q^2)$ as the group of all matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $d = \bar{a}$ and $c = \bar{b}$, where the map $x \mapsto \bar{x}$ is the generator of $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$. Then we may assume that τ_1 is the diagonal matrix $\mathrm{diag}(\zeta, \zeta^{-1})$. Take τ_2 to be

$$\tau_2 = \begin{pmatrix} a & b \\ c & t_2 - a \end{pmatrix}.$$

Since the product of the τ_i's is 1, this gives $t_3 = \mathrm{tr}(\tau_3) = \zeta a + \zeta^{-1}(t_2 - a)$. This determines a. Then the product bc is determined by the condition $\det(\tau_2) = 1$. Since τ_1, τ_2, τ_3 do not have a common eigenvector, we have $bc \neq 0$. These conditions determine the matrix τ_2 up to conjugacy by diagonal matrices (which centralize τ_1): This is clear if $\zeta \in \mathbf{F}_q$. In the other case, note that the norm $b\bar{b} = bc$ of b over $\mathbf{F}_q$ is determined by the above conditions. Since the diagonal matrix $\mathrm{diag}(\eta, \bar{\eta})$ conjugates τ_2 into a matrix with right upper entry $\eta^{-1}\bar{\eta}b$, and since every element of $\mathbf{F}_{q^2}$ of norm 1 is of the form $\eta^{-1}\bar{\eta}$, it follows that τ_2 is determined up to conjugacy by matrices $\mathrm{diag}(\eta, \bar{\eta})$. This completes the proof of (a).

Proof of (b). Let α be any automorphism of the field $\mathbf{F}_q$ that fixes t_1, t_2, t_3, and let $\bar{\alpha}$ denote the automorphism of $\mathrm{SL}_2(q)$ induced by α. If (τ_1, τ_2, τ_3) is a triple as in (a), then $\bar{\alpha}$ maps this triple to another one with the same properties. By (a) it follows that $\bar{\alpha}$ has the same effect on this triple as some automorphism β induced by $\mathrm{GL}_2(q)$. Now if $\langle \tau_1, \tau_2, \tau_3 \rangle = \mathrm{SL}_2(q)$, then it follows that $\bar{\alpha} = \beta$. Thus $\bar{\alpha}$ preserves the trace of the elements of $\mathrm{SL}_2(q)$, and so α is trivial. That is, each automorphism of $\mathbf{F}_q$ that fixes t_1, t_2, t_3 is trivial, which proves $\mathbf{F}_p(t_1, t_2, t_3) = \mathbf{F}_q$. □

BIBLIOGRAPHY

[RGTY] M. Aschbacher et al., (eds.), *Proceedings of the Rutgers group theory year* 1983/84, Cambridge Univ. Press, 1984.

[CP] J. H. Conway and R. A. Parker, *On the Hurwitz number of arrays of group elements*, preprint.

[Fr1] M. D. Fried, *Fields of definition of function fields and Hurwitz families - groups as Galois groups*, Comm. Algebra **5** (1977), 17–82.

[Fr2] ——, *Arithmetic of* 3 *and* 4 *branch point covers*, Adv. in Math., Birkhäuser, 1989, pp. 1–33.

[FrTh] M. D. Fried and J. G. Thompson, *The Hurwitz monodromy group* $H(4)$ *and modular curves*, preprint.

[FrVo] M. D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, preprint.

[Fl] W. Feit, *Rigidity of* $\mathrm{Aut}(\mathrm{PSL}_2(p^2))$, $p \equiv \pm 2 (\mathrm{mod}\ 5)$, Proceedings of the Rutgers Group Theory Year 1983/84 (M. Aschbacher et. al., eds.), Cambridge Univ. Press, 1984.

[F2] ——, *Some finite groups with non-trivial centers which are Galois groups*, Proceedings of the 1987 Singapore Group Theory Conference De Gruyter, 1989, pp. 87–109.

[FF] W. Feit and P. Fong, *Rational rigidity of* $G_2(p)$ *for any prime* $p > 5$, Proceedings of the Rutgers Group Theory Year 1983/84 (M. Aschbacher et al., eds.), Cambridge Univ. Press, 1984, pp. 323–326.

[HS] G. Hoyden-Siedersleben, *Realisierung der Jankogruppen* J_1 *und* J_2 *als Galoisgruppen über* $\mathbf{Q}$, J. Algebra **97** (1985), 14–22.

[Hu] B. Huppert, *Endliche Gruppen* I, Springer–Verlag, Berlin-Heidelberg-New York, 1967.

[Hunt] D. C. Hunt, *Rational rigidity and the sporadic groups*, J. Algebra **99** (1986), 577–592.

[Malle1] G. Malle, *Exceptional groups of Lie type as Galois groups*, J. Reine Angew. Math. **392** (1988), 70–109.

[Malle2] ——, *Some unitary groups as Galois groups over* $\mathbf{Q}$, preprint.

[Malle3] ——, *Realisierung von Gruppen* $\mathrm{PSL}_2(q)$ *and* $\mathrm{SL}_2(q)$ *als Galoisgruppen über* $\mathbf{Q}$, Diplomarbeit, Karlsruhe, 1984.

[MM] G. Malle and B. H. Matzat *Realisierung von Gruppen* $PSL_2(\mathbf{F}_p)$ *als Galoisgruppen über* $\mathbf{Q}$, Math. Annalen **272** (1985), 549–565.

[Ma1] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math., vol. 1284, Springer-Verlag, Berlin and New York, 1987.

[Ma2] ——, *Zwei Aspekte konstruktiver Galoistheorie*, J. Algebra **96** (1985), 499–531.

[Sh] K. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Annalen **207** (1974), 99–120.

[Th1] J. G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$, *where* $K \subset \mathbf{Q}(\mu_n)$, J. Algebra **89** (1984), 437–449.

[Th2] ——, PSL_3 *and Galois groups over* $\mathbf{Q}$, Proceedings of the Rutgers Group Theory Year 1983/84 (M. Aschbacher et al., eds.), Cambridge Univ. Press, pp. 309–319.

[Th3] ____, *Primitive roots and rigidity*, Proceedings of the Rutgers Group Theory Year 1983/84 (M. Aschbacher et al., eds.), Cambridge Univ. Press, pp. 327–350.

[Th4] ____, *Rational rigidity of* $G_2(5)$, Proceedings of the Rutgers Group Theory Year 1983/84 (M. Aschbacher et al., eds.), Cambridge Univ. Press, pp. 321–322.

MATHEMATICS DEPARTMENT, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA 36211, USA AND UNIVERSITÄT ERLANGEN

E-mail address: helmut@math.ufl.edu