ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 3, Summer 1989

GROUPS OF SMALL ORDER AS GALOIS GROUPS OVER Q

JACK SONN

1. Introduction. There has been some striking progress recently on the problem of realizing finite nonsolvable groups, especially simple groups, such as Galois groups, over the rationals $\mathbf{Q}$ and over arbitrary number fields [**5a, 6a, 8a, 13, 13a, 13b, 14a, 25a**]. (See [**5a, 13a, 13b**] and the references cited there.)

On the other hand, it is a humbling exercise to try to realize certain nonsolvable groups of small order. For example, the binary icosahedral group $A_5^+ \simeq \mathrm{SL}(2,5)$ (of order 120) was not realized over $\mathbf{Q}$ until 1980 [**25**], and had apparently been known for some time to be the smallest group not realized over $\mathbf{Q}$ since Shafarevich's realization of solvable groups in 1954 [**21**]. A_5^+ was realized over $\mathbf{Q}$ by means of a generalized Laguerre polynomial with Galois group A_5 [**25**]; Schur [**17**] computed Galois groups of certain generalized Laguerre polynomials and other special polynomials, and obtained polynomials with Galois group $A_n, n \neq 4m+2$. The realization in [**25**] was achieved by choosing a realization of A_5 over $\mathbf{Q}$ which could be embedded into an A_5^+-extension of $\mathbf{Q}$ using a local-global principle for the embedding problem. In 1984 Serre [**19a**] discovered a formula relating the obstruction to embedding problems of this type (involving double covers such as $A_5^+ \to A_5$, $A_n^+ \to A_n$, etc.) to the Witt invariant of a trace quadratic form. Recently Feit [**5a**] computed the Witt invariants of generalized Laguerre polynomials and realized A_5^+ and A_7^+ over every number field, as well as A_n^+ over $\mathbf{Q}$ for $n \equiv 3 (\mathrm{mod}\, 4)$. Also Vila [**26a**] has realized A_n^+ over $\mathbf{Q}(t)$ for most $n \equiv 0,1,2,3 (\mathrm{mod}\, 8)$, also using Serre's formula. In [**25**], the author's motivation in realizing A_5^+ over $\mathbf{Q}$ was the fact that if A_5^+ and S_5^+ (one of the two double covers of S_5) are Galois groups over a number field k, then so is every Frobenius group. The realizations of A_5^+ and S_5^+ in [**25**] were obtained from individual polynomials and did not imply the Frobenius group result over all number fields. In [**25a**], the author, using Serre's formula and Feit's computation of the

This research was supported by the Fund for the Promotion of Research at the Technion.

Witt invariants of generalized Laguerre polynomials, realized the two double covers S_5^+, S_5^- of S_5 over all number fields, which, together with Feit's result, implies that every Frobenius group is realizable over every number field. In addition, Schacher and the author, using Serre's computation of the Witt invariants of trinomials with linear term $x^n + ax + b$, have proved that both double covers S_n^+, S_n^- of S_n, are realizable over every number field for $n \equiv 0, 1, 2, 3 \pmod 8$, S_n^+ is realizable for $n \equiv 6, 7 \pmod 8$, and S_n^- for $n \equiv 4, 5 \pmod 8$ [**14b**]. (For definitions of S_n^+, S_n^- see [**25a, 14b**].)

Zeh-Marschke [**27a**] has announced the realization of $\mathrm{SL}(2,7)$ (of order 336) over $\mathbf{Q}$, using a two parameter family of polynomials with Galois group $\mathrm{PSL}(2,7)$ discovered by Lamacchia [**11a**], and finding several specializations with vanishing Witt invariants. The group $\mathrm{PGL}(2,7)$ has been realized for a long time (see [**12**]), but its three nontrivial central extensions by $\mathbf{Z}/2\mathbf{Z}$ (of order 672) have not. For $p > 7$, the latter remains true, but $\mathrm{SL}(2,p)$ has not yet been realized over $\mathbf{Q}$, although $\mathrm{PSL}(2,p)$ has been realized over $\mathbf{Q}$ if 2, 3 or 7 is a quadratic nonresidue $\bmod\, p$ [**23**], or $p \neq \pm 1 \pmod{24}$ [**13**].

In order to satisfy our curiosity (and hopefully the reader's as well), we have proved the following theorem, which asserts that, at present, the smallest fugitives from realizability over $\mathbf{Q}$ are the nontrivial central extensions of $\mathrm{PGL}(2,7)$ mentioned above.

THEOREM 1. *Every group of order less than* 672 *is a Galois group over* $\mathbf{Q}$.

REMARK. In reality, the most difficult part of the proof is the solvable case,due to Shafarevich [**21**] (just contemplate groups of order 2^n). Our discussion here will center about groups having A_5 as their single composition factor, illustrating some of the obstacles encountered in realizing composite nonsolvable groups of small order.

2. Preliminaries. We collect a few known facts which will be used in the proof of Theorem 1. In what follows, C_n denotes a cyclic group of order n. If A is G-module, $H^2(G,A)$ denotes the n^{th} cohomology group of G over A.

LEMMA 2. *Let G be a nonabelian simple group (or any group which coincides with its commutator subgroup) acting trivially on $\mathbf{Z}/n\mathbf{Z}$. Then $H^2(G, \mathbf{Z}/n\mathbf{Z}) \simeq H^2(G, \mathbf{C}^*)_n =$ the subgroup of elements of order dividing n of the Schur multipier $H^2(G, \mathbf{C}^*)$ of G.*

PROOF. Considering $\mathbf{C}^*$ (multiplicative group of the complex numbers $\mathbf{C}$) as trivial G-module, and identifying $\mathbf{Z}/n\mathbf{Z}$ with the n^{th} roots of unity, the short exact sequence

$$0 \to \mathbf{Z}/n\mathbf{Z} \to \mathbf{C}^* \xrightarrow{n} \mathbf{C}^* \to 1$$

yields the cohomology sequence

$$0 = H^1(G, \mathbf{C}^*) \to H^2(G, \mathbf{Z}/n\mathbf{Z}) \to H^2(G, \mathbf{C}^*) \xrightarrow{n} H^2(G, \mathbf{C}^*)$$

which proves the lemma. □

If $1 \to N \to E \to G \to 1$ is an exact sequence of groups, we will say that E is an extension of G by N. $\operatorname{Aut} N$, $\operatorname{Inn} N$ and $\operatorname{Out} N$ will denote the automorphism group of N, the inner automorphism group of N, and the outer automorphism group $\operatorname{Aut} N/\operatorname{Inn} N$, respectively, and $Z(N)$ will denote the centre of N. We will use the following description of the extensions of G by N, due to Baer [**2**] (see [**11**]).

The action of E on N by conjugation induces a homomorphism

$$\psi : G \to \operatorname{Out} N$$

as well as an action of G on $Z(N)$, relative to which we may form $H^2(G, Z(N))$.

LEMMA 3. *Given $\psi : G \to \operatorname{Out} N$, the number of inequivalent extensions of G by N inducing ψ is either zero or the order of $H^2(G, Z(N))$.*

For the proof see [**11**, p. 194].

Given epimorphisms of groups $a : A \to C, b : B \to C$, the *pullback* G of a, b is the subgroup of $A \times B$ consisting of all pairs (x, y), such that $a(x) = b(y)$. G is an extension of C by $\ker(a) \times \ker(b)$ and G is an extension of A by $\ker(b)$ and of B by $\ker(a)$. Similarly define the *pushout* H of monomorphisms $a : C \to A$, $b : C \to B$ as the factor group of $A \times B$ modulo the diagonal subgroup $\{(a(x), b(x)) : x \in C\}$. If $a(C) \triangleleft A$ and $b(C) \triangleleft B$, then H is an extension of $\operatorname{coker}(a) \times \operatorname{coker}(b)$ by C, and H is an extension of $\operatorname{coker}(a)$ by B and of $\operatorname{coker}(b)$ by A.

The pullback G of a, b has the following universal mapping property: If G_1 is any group and $r : G_1 \to A$, $s : G_1 \to B$ are epimorphisms such that $ar = bs$, then there exists an epimorphism $t : G_1 \to G$. An analogous property holds for pushouts.

REMARK 4. Let $1 \to N \xrightarrow{i} E \xrightarrow{e} G \to 1$ define a group extension of G by N. Suppose N has trivial center. Then the map i and conjugation inside E defines a homomorphism $a : E \to \operatorname{Aut} N$ whose kernel M is the centralizer of iN in E. Thus $M \cap iN = 1$, and we obtain the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{e} & G \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle b} \\ a(E) & \xrightarrow{\text{can}} & b(G) \end{array}$$

where b is chosen to make the diagram commute, and can is the canonical map from $\operatorname{Aut} N$ to $\operatorname{Out} N$. It follows, from the universal mapping property of pullbacks and the fact that the pullback P of

$$G \to b(G) \leftarrow a(E)$$

has the same order as E, that $P \simeq E$.

REMARK 5. Given a field k and a finite Galois extension K/k, an epimorphism $e : E \to G(K/k)$, with E a finite group, is said to define an *embedding problem* over K/k. A *solution* is a Galois extension L of k containing K and an isomorphism $f : G(L/k) \to E$ such that $e \cdot f = \operatorname{res}(L/K)$, the restriction map.

Let $e : E_i \to G(K/k)$, $i = 1, 2$ be two embedding problems over K/k, and let $f_i : G(L/k) \to E_i$ be respective solutions. If

$L_1 \cap L_2 = K$, then $G(L_1L_2/k)$ is isomorphic to the pullback of the maps $e_i : E_i \to G(K/k)$, $i = 1, 2$. Conversely, if G is a pullback of epimorphisms $e_i : E_i \to F$, and if $G(M/k) \simeq G$, then $M = L_1L_2$, where L_i are Galois over k, $i = 1, 2$, $G(L_i/k) \simeq E_i$ and $G(L_1 \cap L_2/k) \simeq F$. In the degenerate case $L_1 \cap L_2 = k$ if and only if $G(L_1L_2/k) \simeq E_1 \times E_2$.

3. Proof of Theorem 1. By virtue of Shafarevich's theorem [**21**], we may confine ourselves to nonsolvable groups G of order less than 672. It is clear that G has exactly one nonabelian composition factor since 60 is the order of the smallest nonabelian simple group A_5. The next simple group in order of size is $\mathrm{PSL}(2,7)$ of order 168; the third is A_6 of order 360; the fourth is $\mathrm{PSL}(2,8)$ of order 504, the last of order < 672.

If G has $\mathrm{PSL}(2,8)$ as composition factor, then $G \simeq \mathrm{PSL}(2,8)$ which is realized over $\mathbf{Q}$ [**13**, p.209]. The same is true for A_6 by [**7**]. If G has composition factor $\mathrm{PSL}(2,7)$, then either $G = \mathrm{PSL}(2,7)$ which is realizable [**23**; 27, p. 12], or contains $\mathrm{PSL}(2,7)$ as a subgroup of index 2, or G has a center C of order 2, with $G/C \simeq \mathrm{PSL}(2,7)$.

Suppose first that G contains $N \simeq \mathrm{PSL}(2,7)$ of index 2. Since $Z(N) = 1$, it follows from Lemma 3 that, for each homomorphism $\psi : G/N \to \mathrm{Out}\, N$, there is at most one extension of $G/N \simeq C_2$ by N. Now, $\mathrm{Out}\, N \simeq C_2$ since $\mathrm{Aut}\, N \simeq \mathrm{PGL}(2,7)$ [**16, 5**], hence there are exactly two extensions G of C_2 by $\mathrm{PSL}(2,7)$, namely $C_2 \times \mathrm{PSL}(2,7)$ and $\mathrm{PGL}(2,7)$. The first is clearly realizable since $\mathrm{PSL}(2,7)$ is, and $\mathrm{PGL}(2,7)$ is realizable by Weber-Macbeath [**12**].

Suppose next that G is an extension of $\mathrm{PSL}(2,7)$ by C_2. Such extensions are described by $H^2(\mathrm{PSL}(2,7), \mathbf{Z}/2\mathbf{Z})$ [**9**, p. 120]. The Schur multiplier $H^2(\mathrm{PSL}(2,7), \mathbf{C}^*)$ of $\mathrm{PSL}(2,7)$ is $\mathbf{Z}/2\mathbf{Z}$ [**9**, p. 646], hence by Lemma 2, $H^2(\mathrm{PSL}(2,7), \mathbf{Z}/2\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$, so the only extensions of $\mathrm{PSL}(2,7)$ by C_2 are the direct product and $\mathrm{SL}(2,7)$.

It remains to consider G having A_5 as a composition factor. Then $|G| = 60.n, 1 \le n \le 11$. We consider several cases.

Case 1. G is an extension of a group H (of order n) by A_5. $\mathrm{Out}\, A_5 \simeq C_2$ [**18**, p. 314], so, by Remark 4, G is either the direct product $H \times A_5$ or G is a pullback of $H \to C_2 \leftarrow S_5$. $H \times A_5$ is clearly realizable since both H and A_5 are. In the latter case, H has order 2, 4, 6, 8, or 10. If H has order 2, then $G \simeq S_5$ is realizable. There are two groups of order 4, two of order 6, 5 of order 8, and 2 of order 10; and all are realizable. By Remark 5, an extension with Galois group G is a composite of two Galois extensions $K/\mathbf{Q}$ and $L/\mathbf{Q}$ with $G(K/\mathbf{Q}) \simeq S_5$, $G(L/\mathbf{Q}) \simeq H$, and $K \cap L = \mathbf{Q}(\sqrt{d}) \neq \mathbf{Q}$ for some $d \in \mathbf{Q}$. Gaddis [**6**] has proved that any quadratic field $\mathbf{Q}(\sqrt{d}), d \neq -1$, can be embedded into an S_n extension, for any $n > 2$. It suffices therefore to show that, for each H, there exists a Galois extension $L/\mathbf{Q}$ with $G(L/\mathbf{Q}) \simeq H$ and such that every quadratic subfield of L is of the form $\mathbf{Q}(\sqrt{d})$, where $d \neq -1$:

$$
\begin{array}{ll}
\text{For } H = C_2 \times C_2, & L = \mathbf{Q}(\sqrt{2}, \sqrt{3}); \\
\text{For } H = C_4, & L = \mathbf{Q}(e^{2\pi i/5}) \supseteq Q(\sqrt{5}; \\
\text{For } H = C_6, & L = \mathbf{Q}(e^{2\pi i/7}) \supseteq Q(\sqrt{-7}); \\
\text{For } H = S_3, & L = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2}); \\
\text{For } H = C_8, & L = \mathbf{Q}(e^{2\pi i/17} + e^{-2\pi i/17}); \\
\text{For } H = C_4 \times C_2, & L = \mathbf{Q}(\sqrt{2}), e^{2\pi i/5}); \\
\text{For } H = C_2 \times C_2 \times C_2, & L = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}).
\end{array}
$$

For $H = D_8$ (the dihedral group) or Q_8 (the quaternion group), it is an old fact that if $p \neq q$ are primes $\equiv 1 (\bmod 4)$ and p is a quadratic residue $\bmod q$ (say $p = 29, q = 5$), then $\mathbf{Q}(\sqrt{p}, \sqrt{q})$ can be embedded into both D_8 and Q_8 extensions (see, e.g., [**20**]: $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ is Scholz with respect to 4). For $C_{10}, L = \mathbf{Q}(e^{2\pi i/11})$. For the dihedral group D_{10} of order 10, we resort to Scholz's theorem [**15**; **8**, p. 100], which implies that any quadratic extension is embeddable into a D_{10}-extension. This completes Case 1.

Case 2. G is an extension of A_5 by a group N of order $\leq$ 11. By Lemma 3, these extensions are characterized by elements of $\operatorname{Hom}(A_5, \operatorname{Out} N) \times H^2(A_5, Z(N))$. We first observe that, for groups N of order ≤ 11, $\operatorname{Hom}(A_5, \operatorname{Out} N) = 0$. Indeed it is easy to check that, in every case except $C_2 \times C_2 \times C_2$, $\operatorname{Aut} N$ is solvable, which suffices. $\operatorname{Aut}(C_2 \times C_2 \times C_2) \simeq \mathrm{GL}(3,2)$, the simple group of order 168. Since 168 is not divisible by 60, $\operatorname{Hom}(A_5, \operatorname{Out}(C_2 \times C_2 \times C_2) = 0$. It follows that these extensions are characterized by elements of $H^2(A_5, Z(N))$, with A_5 acting trivially on $Z(N)$. For N abelian, G is a central extension of A_5 by N, which is always realizable over $\mathbf{Q}$ [**25**; Corollary, Theorem 3]. For $N = S_3, Z(S_3) = 1$ so $G \simeq A_5 \times S_3$. This leaves $N = D_8, Q_8$ and D_{10}, all having center C_2. By [**9**, p. 646], the Schur multiplier $H^2(A_5, C^*) = H^2(\mathrm{PSL}(2,5), C^*) \simeq \mathbf{Z}/2\mathbf{Z}$, so, by Lemma 2, $H^2(A_5, \mathbf{Z}/2\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$. Thus, in addition to the direct products $N \times A_5$, we get the pushouts $N \to C_2 \leftarrow \mathrm{SL}(2,5)$, which are factor groups of $N \times \mathrm{SL}(2,5)$, and hence realizable over $\mathbf{Q}$. This completes Case 2.

Case 3. A_5 is neither a subgroup nor a factor group of G. This is possible only for $n = 4$ or 8. In every case, G acts on the invariant composition factor A_5 by inner automorphisms, so there is induced a homomorphism of G into $\mathrm{Aut}\, A_5 \simeq S_5$ which, by our present hypothesis, must be surjective. Hence G is an extension of S_5 by a (sub)group N of order 2 or 4. If $N \simeq C_2$, then, by [**25**, Theorem 2], G is realizable over $\mathbf{Q}$. There are in fact four nonisomorphic extensions of S_5 by C_2.

The remaining case is when G is an extension of S_5 by a group N of order 4. This extension does not split since, by hypothesis, A_5 is not a subgroup of G. Suppose that G contains a subgroup U of index 2 such that $UN = G$. Then U is an extension of S_5 by C_2 and so realizable. U acts on N by conjugation inside G. Let $U \cdot N$ be the semidirect product of U and N with this action. By Scholz's theorem [**15**; **8**, p. 100], $U \cdot N$ is realizable, hence so is G, which is a homomorphic image of $U \cdot A$ under the map $(u, a) \to ua$.

We may therefore assume that the only subgroup U of G, such that $UN = G$ is $U = G$. G has a unique subgroup H of index 2 containing N, and $H/N \simeq A_5$. Since A_5 acts trivially on N, H is a central extension of A_5 by N. By hypothesis, H does not have A_5 as a subgroup, so, by [**25**, proof of Corollary to Theorem 3], H has a subgroup $U \simeq \mathrm{SL}(2,5)$ such that $UN = H$. U is clearly normal in G, so G is an extension of a group B of order 4 by $U \simeq \mathrm{SL}(2,5)$. If $B \simeq C_2 \times C_2$ is in the kernel, then G has three distinct subgroups of index 2, only one of which contains N, namely H. Let H' be another. Then $H'N > H'$; hence $H'N = G$, contrary to hypothesis. We may therefore assume that $B \simeq C_4$. We apply Lemma 3. Now $\mathrm{Aut}\,\mathrm{PSL}(2,5) \simeq \mathrm{Aut}\, A_5 \simeq S_5 \simeq \mathrm{PGL}(2,5)$. Furthermore, $\mathrm{Aut}\,\mathrm{SL}(2,5) = \mathrm{Aut}\,\mathrm{PSL}(2,5)$. (Indeed, every automorphism of $\mathrm{SL}(2,5)$ induces one on $\mathrm{PSL}(2,5)$, so we have a natural homomorphism from $\mathrm{Aut}\,\mathrm{SL}(2,5)$ to $\mathrm{Aut}\,\mathrm{PSL}(2,5)$ which is clearly surjective.

If $\sigma \in \operatorname{Aut} \mathrm{SL}(2,5)$ is in the kernel then, for every $x \in \mathrm{SL}(2,5), x^\sigma = \varepsilon(x) \cdot x$, $\varepsilon(x) = \pm 1$. $\varepsilon : \mathrm{SL}(2,5) \to \{\pm 1\}$ is a homomorphism which is necessarily trivial, since $\mathrm{SL}(2,5)$ coincides with its commutator subgroup.) It follows that $\operatorname{Out} \mathrm{SL}(2,5) \simeq \mathrm{PGL}(2,5)/\mathrm{PSL}(2,5) \simeq C_2$. Now $\operatorname{Hom}(B, \operatorname{Out} \mathrm{SL}(2,5)) \simeq \operatorname{Hom}(C_4, C_2) \simeq \mathbf{Z}/2\mathbf{Z}$.

The trivial homomorhpism implies that $\mathrm{PSL}(2,5) \simeq A_5$ is a factor group of G, contrary to hypothesis, hence there is only one homomorphism (nontrivial) to consider. Corresponding to this homomorphism, we compute $H^2(B, Z(\mathrm{SL}(2,5)) \simeq H^2(C_4, \mathbf{Z}/2\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$. By Lemma 3 there are at most two extensions of C_4 by $\mathrm{SL}(2,5)$ to consider. One such extension is $\mathrm{GL}(2,5)$, which is realizable over $\mathbf{Q}$ [**19**, p. 21]. (It is in fact an essential extension of S_5 by C_4. For, if $\mathrm{GL}(2,5)$ contained a proper subgroup U such that $UZ = \mathrm{GL}(2,5)$, where $Z = Z(\mathrm{GL}(2,5))$, U would necessarily contain $\mathrm{SL}(2,5)$ and would therefore have to be $\mathrm{SL}(2,5)$ or $Z \cdot \mathrm{SL}(2,5)$, neither of which satisfy $UZ = \mathrm{GL}(2,5)$.)

The other extension is the pullback G of $S_5^+ \to C_2 \leftarrow C_4$, where S_5^+ is the central extension of S_5 by C_2 whose Sylow 2-subgroup is the generalized quaternion group of order 16 [**24**, Lemma 2.6]. G is not isomorphic to $\mathrm{GL}(2,5)$ since $\mathbf{Z}(G) \simeq C_2 \times C_2$ and $\mathbf{Z}(\mathrm{GL}(2,5)) \simeq C_4$. To realize G over $\mathbf{Q}$, let K be the splitting field of

$$f(x) = x^5 + 2x^4 - 3x^3 - 5x^2 + x + 1.$$

$G(K/\mathbf{Q}) \simeq S_5$ and K is embeddable into an extension $L = K(\sqrt{\alpha})$ such that $G(L/\mathbf{Q}) \simeq S_5^+$ [**25**, Theorem 2]. The unique quadratic subfield of K is $\mathbf{Q}(\sqrt{D})$, where $D = 36,497$, a prime $\equiv 1 (\operatorname{mod} 4)$. Therefore $\mathbf{Q}(\sqrt{D})$ is embeddable into a cyclic quartic subfield M of the field of D^{th} roots of unity. By Remark 5, $G(ML/\mathbf{Q}) \simeq G$.

This completes the proof of Case 3 and of Theorem 1. □

Added in Proof. J.F. Mestre has proved that $\tilde{A}_n = A_n^+$ is realizable over every number field for all n.

REMARK. It has not been proved that the group G in the last paragraph is realizable over every number field.

REFERENCES

1. E. Artin, *The orders of the classical simple groups,* Com. Pure Appl. Math. **8** (1955), 455-472.

2. R. Baer, *Erweiterung von Gruppen und ihren Isomorphismen,* Math. Z. **38** (1934), 375-416.

3. C. Chevalley, *Invariants of finite groups generated by reflections,* Amer. J. Math. **77** (1955), 778-782.

4. L.E. Dickson, *Linear Groups,* Dover, 1958.

5. J. Dieudonné, *On the automorphisms of the classical groups,* Mem. A.M.S. **2** (1951), 1-95.

5a. W. Feit, *$\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields,* preprint.

6. T. Gaddis, *G-closed fields and imbedding of quadratic number fields,* J. Number Th. **8** (1976), 58-72.

6a. D. Gorenstein, *Classifying the finite simple groups,* Bull. A.M.S. (New Series) **14** (1986), 1-98.

7. D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen,* J.R. Ang. Math. **110** (1892), or Ges. Abh II, 264-286.

8. K. Hoechsmann, *Zum Einbettungsproblem,* J.R. Ang. Math. **229** (1968), 81-106.

8a. G. Hoyden and B.H. Matzat, *Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilunskörpern,* J. Algebra, to appear.

9. B. Huppert, *Endliche Gruppen* I., Springer-Verlag, 1967.

10. V.V. Ishkhanov, *On the semidirect imbedding problem with nilpotent kernel,* Math. USSR. **10** (1976), 1-23.

11. C.E. Johnson, H. Zassenhaus, *On equivalence of finite group extensions,* Math. Z. **123** (1971), 191-200.

11a. S.E. LaMacchia, *Polynomials with Galois group* PSL(2, 7), Comm. Alg. **8** (1980), 983-992.

12. A.M. Macbeath, *Extensions of the rationals with Galois group* $\mathrm{PGL}(2, \mathbf{Z}_n)$, Bull. London Math. Soc. **1** (1969), 332-338.

13. B.H. Matzat, *Konstruktion von Zahl-und Funktionen körpern mit vorgegebener Galoisgruppe,* J.R. Ang. Math. **349** (1984), 179-220.

13a. ———, *Realisierung endlicher gruppen als Galoisgruppen,* Manusc. Math. **51** (1985), 253-265.

13b. ———, *Über das Umkehrproblem der galoisschen Theorie,* Lecture at the 1985 Austrian Math. Congress.

14. E. Noether, *Gleichungen mit vorgeschriebener gruppe,* Math. Ann. **78** (1916), 221-229.

14a. K.A. Ribet, *On ℓ-adic representations attached to modular forms,* Inv. Math. **28** (1975), 245-275.

14b. M. Schacher and J. Sonn, *Double covers of the symmetric groups as Galois groups over number fields* (preprint).

15. A. Scholz, *Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoissche Gruppe,* Math. Z. **30** (1929), 332-356.

16. O. Schreier, and B.L. Van der Waerden, *Die Automorphismen der Projectiven gruppen,* Abh. Math. Sem. Hamburg **6** (1928), 303-332.

17. J. Schur, *Affectlöse Glechungern in der theorie der Laguerreschen und Hermiteschen Polynome,* J.R. Ang. Math. **165** (1931), 52-58.

18. W.R. Scott, *Group Theory,* Prentice-Hall, 1964.

19. J.P. Serre, *Abelian ℓ-adic representations and elliptic curves,* Benjamin, N.Y., 1968.

19a. ———, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comm. Math. Helv. **59** (1984), 651-676.

20. I.R. Shafarevich, *On Construction of fields with a given Galois group of order ℓ^{th}*, A.M.S. Transl. (2) **4** (1956), 107-142.

21. ———, *Construction of fields of algebraic numbers with given solvable Galois group,* A.M.S., Transl. (2) **4** (1956), 185-237.

22. ———, *The imbedding problem for splitting extensions* (Russian) Dokl. Akad. Nauk SSSR **128** (1958), 1217-1219.

23. K.Y. Shih, *On the construction of Galois extensions of function fields and number fields,* Math. Ann. **207** (1974), 99-120.

24. J. Sonn, *Frobenius Galois groups over quadratic fields,* Israel J. Math. **31** (1978), 91-96.

25. ———, $\mathrm{SL}(2,5)$ *and Frobenius Galois groups over* $\mathbf{Q}$, Can. J. Math. **32** (1980), 281-293.

25a. ———, *Double covers of S_5 and Frobenius groups as Galois groups over number fields* (preprint).

26. B.L. Van derWaerden, *Modern Algebra,* Vol. I, Ungar, N.Y., 1949.

26a. N. Vila, *On central extensions of A_n as Galois groups over* $\mathbf{Q}$, Arch. Math. **44** (1985), 424-437.

27. H.G. Zimmer, *Computational problems, methods and results in algebraic number theory,* Lecture Notes in Math., Springer, New York, 1972.

27a. A. Zeh-Marschke, $\mathrm{SL}_2(7)$ *als Galoisgruppe über* $\mathbf{Q}$, preprint, 1987.

FACULTY OF MATHEMATICS, TECHNION-ISRAEL, INSTITUTE OF TECHNOLOGY, HAIFA, 32000 ISRAEL