Central Extensions of Symmetric Groups as Galois Groups

D. KOTLAR
Department of Mathematics, Technion, Israel Institute of Technology, Haifa, Israel

M. SCHACHER
Department of Mathematics, University of California, Los Angeles, California 90024

AND

J. SONN
Department of Mathematics, Technion, Israel Institute of Technology, Haifa, Israel

Communicated by Walter Feit
Received March 17, 1988

INTRODUCTION

This paper is in the spirit of [2] and [4]. We are concerned with applications of a theorem of Serre, which relates the obstruction to the embedding problem:

$$S_n^- \rightarrow S_n \cong G(K/k)$$

to the Witt invariant of a trace form. Here $S_n^-$ is one of the double covers of the symmetric group $S_n$, and $G(K/k)$ is the Galois group of a Galois extension $K$ of the field $k$.

We review briefly the theory of the double covers of the group $S_n$, along with the construction of the covers $S_n^+$ and $S_n^-$. 

1 Supported in part by the Wolf Foundation.
2 Supported in part by NSF Grant DMS85-00929. During this work, Murray Schacher was also a Fulbright-Hayes Fellow in Belgium under the auspices of the Commission for Educational Exchange Between the United States, Belgium, and Luxembourg.
$S_n$ has a standard presentation with generators $t_1, t_2, ..., t_{n-1}$ ($t_i$ is the transposition $(i, i + 1)$) and relations

$$
t_i^2 = 1, \quad i = 1, 2, ..., n-1
$$

$$(t_i t_{i+1})^3 = 1, \quad i = 1, 2, ..., n-2
$$

$$t_i t_j = t_j t_i, \quad i = 1, 2, ..., n-2, j \geq i + 2.
$$

For the corresponding presentation for $S_n^+$, there are generators $a, x_1, x_2, ..., x_{n-1}$ and relations

$$
a^2 - 1, \quad x_i^2 - a, \quad 1 \leq i \leq n-1
$$

$$(x_i x_{i+1})^3 = 1, \quad 1 \leq i \leq n-2
$$

$$x_i x_j = ax_j x_i, \quad 1 \leq i \leq n-2, j \geq i + 2.
$$

For the presentation for $S_n^-$, there are generators $b, y_1, y_2, ..., y_{n-1}$ and relations

$$
b^2 = 1, \quad y_i^2 = 1, \quad 1 \leq i \leq n-1
$$

$$(y_i y_{i+1})^3 = 1, \quad 1 \leq i \leq n-2
$$

$$y_i b = by_i, \quad i = 1, 2, ..., n-1
$$

$$y_i y_j = by_j y_i, \quad 1 \leq i \leq n-2, j \geq i + 2.
$$

The maps $x_i \to t_i$ (resp. $y_i \to t_i$) show that $S_n$ is a homomorphic image of $S_n^+$ (resp. $S_n^-$) with kernel the central subgroup of order 2 generated by $a$ (resp. $b$).

There are two other double covers of $S_n$ in this sense: the direct product $S_n \times \mathbb{Z}/2\mathbb{Z}$, and the pullback of the diagram $S_n \to \mathbb{Z}/2\mathbb{Z} \leftarrow \mathbb{Z}/4\mathbb{Z}$, where the maps in question are the uniquely determined surjective maps. (See [5].)

The main result of [4] was:

**Theorem A.** Let $n$ be a positive integer $\geq 4$.

1. If $n \equiv 0, 1, 2, \text{ or } 3 \pmod{8}$, then both $S_n^+$ and $S_n^-$ are realizable as Galois groups over every number field.

2. If $n \equiv 4$ or $5 \pmod{8}$, then $S_n^-$ is realizable as a Galois group over every number field.

3. If $n \equiv 6$ or $7 \pmod{8}$, then $S_n^+$ is realizable as a Galois group over every number field.

The technique of the proof of Theorem A in [4] was to realize these groups infinitely often over the rational field $\mathbb{Q}$ by a sequence of fields.
which are linearly disjoint, and then conclude that they are realizable over every number field. We sought there to find trinomials with linear term \(x^n + ax + b \in \mathbb{Q}[x]\) whose Galois group is \(S_n\) so that the splitting field is embeddable into an \(S_n^+\) or \(S_n^-\) extension. It is actually proved in [4] that these trinomials cannot serve for the missing cases in Theorem A.

Since \(S_n^+\) and \(S_n^-\) are Galois groups over all number fields by [8], the smallest missing cases in Theorem A are \(S_6^+\) and \(S_7^-\). In fact, the omission of \(S_6^-\) is only apparent, since it was known to Schur (see [5]) that \(S_6^- \cong S_6^+\); such an isomorphism does not occur for any other values of \(n\), and follows from the existence of the outer automorphism of \(S_6\). Thus, \(S_6^-\) is a Galois group over all number fields since \(S_6^+\) is by Theorem A.

In this paper, we will show that \(S_7^-\) is a Galois group over all number fields. The argument closely follows ideas suggested in [2], including the use of Laguerre polynomials and associated geometric methods.

We then consider the question whether all central extensions of \(S_n\) are Galois groups over the rational field \(\mathbb{Q}\). After a reduction to the case of pullbacks, we show that this is true for \(n \leq 6\).

Following the notation of [2], we write \(a \sim b\) if \(a/b\) is a square in a field \(K\). Similarly for vectors we write \((x_1 , x_2 , x_3) \sim (y_1 , y_2 , y_3)\) if \(x_i \sim y_i\) for \(i = 1, 2, 3\).

1. SERRE'S FORMULA

Let \(q\) be a non-degenerate quadratic form in \(n\) variables over a field \(K\) of characteristic \(\neq 2\). We follow the notation in [6]; if \(a, b \in K\), we set \(\{a, b\}\) to be the generalized quaternion algebra generated by elements \(u, v\) over \(K\) subject to \(u^2 = a, v^2 = b, uv = -vu\). We denote by \((a, b)\) the class of \(\{a, b\}\) in \(Br_2(k)\), the elements of order 1 or 2 in the Brauer group of \(K\). The Witt invariant \(w(q)\) of \(q\) is defined by

\[
w(q) = \prod_{i < j} (a_i, a_j),
\]

where \(q \sim a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2\) in diagonalizable form, and \(w(q)\) is regarded as an element in \(Br_2(K)\).

Suppose \(K\) is a field of characteristic \(\neq 2\), and \(f(x) \in K[x]\) is a separable irreducible polynomial of degree \(n\). Let \(E = K[x]/(f(x))\) be the field obtained by adjoining a root of \(f\), and \(q_E(x) = tr_{E/K}(x^2)\) for \(x \in E\); \(q_E\) is the trace quadratic form on \(E\). We set \(L = \text{the splitting field of } f/E\), and \(G = G(L/K)\). Let \(d_E \in K^*/K^{*2}\) be the discriminant of \(E/K\). By context, \(G \subset S_n\), so it makes sense to speak of \(G^+\) (resp. \(G^-\)) as the inverse image of \(G\) under the canonical map \(S_n^+ \to S_n\) (resp. \(S_n^- \to S_n\)). It is known that \(G^+ \cong G^-\) if \(G \subset A_n\), the alternating group. Serre's Theorem says:
THEOREM 1. (1) \( L \) can be extended to a quadratic extension \( L^- \) of \( L \) with \( G(L^-/K) \cong G^- \) so that the restriction map \( G(L^-/K) \to G(L/K) \) is the canonical map \( G^- \to G \) if and only if \( w(q_E)(2, d_E) = 1 \) in \( Br_2(K) \).

(2) \( L \) can be extended to a quadratic extension \( L^+ \) of \( L \) with \( G(L^+/K) \cong G^+ \) so that the restriction map \( G(L^+/K) \to G(L/K) \) is the canonical map \( G^+ \to G \) if and only if \( w(q_E)(-2, d_E) = 1 \) in \( Br_2(K) \).

Part (1) of Theorem 1 is proved in \([6]\). Part (2) follows from the arguments of \([6]\); a complete proof is written out in \([8]\).

2. GENERALIZED LAGUERRE POLYNOMIALS

Let \( \lambda, \mu \) be indeterminates over \( \mathbb{Q} \). For any integer \( i \), let \( c_i = \lambda + i\mu \). Define

\[
F_n(x, \lambda, \mu) = x^n - nc_n x^{n-1} + \left( \begin{array}{c} n \\ 2 \end{array} \right) c_n c_{n-1} x^{n-2} \\
+ \cdots + (-1)^n c_n c_{n-1} \cdots c_1
\]

\[
= \sum_{j=0}^{n} (-1)^n \left( \begin{array}{c} n \\ j \end{array} \right) \left( \prod_{i=j+1}^{n} c_i \right) x^j.
\]

Since \( F_n(x, \lambda, \mu) = \mu^n F_n(x/\mu, \lambda/\mu, 1) \), questions of the Galois group boil down to the case \( \mu = 1 \). If \( \Delta_n(\lambda, \mu) \) denotes the discriminant of \( F_n(x, \lambda, \mu) \), Schur's work gives the formulas presented in \([2]\):

\[
\Delta_n(\lambda, \mu) \sim \begin{cases} \\
\mu^k \prod_{i=1}^{k-1} (1 + 2i) \prod_{i=1}^{k} (\lambda + 2i\mu) & \text{if } n = 2k \\
\mu^k \prod_{i=1}^{k} (1 + 2i) \prod_{i=1}^{k} (\lambda + 2i\mu) & \text{if } n = 2k + 1.
\end{cases}
\]

These formulas remain valid if \( \lambda \) and \( \mu \) are specialized to rational values. Hence

\[
\Delta_n(1, 1) \sim \begin{cases} \\
1 & \text{if } n \text{ is odd} \\
+1 & \text{if } n \text{ is even}.
\end{cases}
\]

Schur studied the polynomials \( F_n(x, 1, 1) \) and showed they are irreducible over \( \mathbb{Q} \) with Galois group \( A_n \) or \( S_n \), depending on whether or not the discriminant is a square. If \( \mu = 1 \), then the form of the discriminant above, as a product of linear terms, is generically not a square in \( \mathbb{Q}(\lambda) \). It follows that \( F_n(x, \lambda, \mu) \) is irreducible over \( \mathbb{Q}(\lambda) \) with Galois group \( S_n \). Since the
associated splitting field is obviously a regular extension of \( Q(\lambda) \) (the normal closure of any algebraic subfield would have to contain the discriminant field), the same conclusion holds if \( Q \) is replaced by any number field \( K \).

3. The Case \( n = 7 \)

We wish to show that \( S_7^- \) is a Galois group over all number fields. We do this by studying appropriate Laguerre polynomials.

Suppose \( F_7(x, \lambda, 1) \) is the Laguerre polynomial of degree 7 in a variable \( \lambda \). Following [2], we set \( t = \lambda + 4 \). Let \( A \) be the discriminant of this polynomial. Then by [2, p. 237],

\[
A \sim 105(t - 2) t(t + 2).
\]

Using [2, p. 254], the Witt invariant of the trace form is

\[
w = \prod_{i=1}^{6} (A_i, A_{i+1})(-1, A_1 A_2 \cdots A_6),
\]

where \( A_1 \sim 7, A_2 \sim 6c_7, A_3 \sim 35c_6, A_4 \sim 6c_5c_7, A_5 \sim 105c_4c_6, A_6 \sim 3c_3c_5c_7, A = A_7 \sim 105c_2c_4c_6 \) and \( c_i = \lambda + i, i = 1, 2, \ldots, 7 \).

Thus the obstruction for the embedding problem relative to \( S_7^- \) is

\[
e = \mathcal{w}(2, A) = \mathcal{w}(2, 105t(t^2 - 4)).
\]  

(3.1)

The value of \( e \) can thus be calculated for any rational \( \lambda \) and \( t = \lambda + 4 \). If we set \( \lambda = 3 \), we get:

**Theorem 2.**  
(1) \( F_7(x, 3, 1) \) is irreducible over \( Q \) with Galois group \( S_7 \).  
(2) The discriminant field of the splitting field of \( F_7(x, 3, 1) \) over \( Q \) is \( Q(\sqrt{3}) \).  
(3) The obstruction \( e \) for \( S_7 \) in (1) vanishes.

**Proof.** Part (1) can be verified by reducing \( F_7(x, 3, 1) \) mod \( p \) for enough primes \( p \). We did this using the computational program "Macsyma." In fact, the polynomial is irreducible (mod 31), and factors (mod 11) as the product of an irreducible quadratic times an irreducible quintic. Thus, the Galois group contains both a 7-cycle and a 2-cycle, and then it follows that it must be \( S_7 \). Part (2) follows since \( (t - 2, t, t + 2) \sim (5, 7, 1) \), and so \( 105t(t^2 - 4) \sim 7 \cdot 5 \cdot 3 \cdot 5 \cdot 7 \cdot 1 \sim 3 \). Part (3) is a routine calculation, using (3.1).
Applying Theorem 1, we get $S_{\gamma}$ is a Galois group over $\mathbb{Q}$ with discriminant field $\mathbb{Q}(\sqrt{3})$. We aim for more.

Consider the elliptic curve $C$ given by

$$3y^2 = 105t(t^2 - 4). \quad (3.2)$$

Evidently, $C$ has the rational point $P = (7, 105)$. Of course (3.2) is equivalent to the equation

$$y^2 = 35(t^3 - 4t)$$

which is equivalent to

$$(35)^2 y^2 = (35)^3 (t^3 - 4t) = (35)^3 t^3 - (35)^3 \cdot 4t.$$  

Making the substitution $Y = 35y$, $T = 35t$ yields an equation for an elliptic curve $\bar{C}$:

$$Y^2 = T^3 - (35)^2 \cdot 4T. \quad (3.3)$$

We get from rational points on $\bar{C}$ to rational points on $C$ by division by 35. $\bar{C}$ has the rational point $\bar{P} = (35 \cdot 7, 35 \cdot 105)$. Equation (3.3) is in nearly Weierstrass normal form, and so we can use the explicit addition and duplication formulas of [3, p. 39401 to calculate multiples of points on $\bar{C}$. A calculation gives

$$2\bar{P} = \left( \frac{(53)^2}{2^2 \cdot 3^2}, \frac{17 \cdot 53 \cdot 73}{2^3 \cdot 3^3} \right).$$

As $2\bar{P}$ is not an integral point, the Lutz–Nagell theorem [3, p. 55] says that $\bar{P}$ has infinite order on $\bar{C}$.

**Lemma 1.** Let $(t, y)$ be a solution of (3.2) which corresponds to an odd multiple of $\bar{P}$ in the correspondence between $C$ and $\bar{C}$. Then $(t - 2, t, t + 2) \sim (5, 7, 1)$ in $(\mathbb{Q}^*)^3$. In particular, there are infinitely many rational numbers $t$ satisfying

$$(t - 2, t, t + 2) \sim (5, 7, 1) \quad (3.4)$$

**Proof.** By (3.3), $Y^2 = T(T - 70)(T + 70)$ for any point $(T, Y)$ on $\bar{C}$. Let $M$ be the multiplicative group of $\mathbb{Q}^*$ mod squares. The map which sends $(T, Y)$ corresponding to a multiple of $\bar{P}$ onto $(T - 70, T, T + 70)$ defines a homomorphism from rational points on the curve onto a finite subgroup of $M^3$ (see [3, pp. 101–105]). Let $P_1$ be the point corresponding to $(175, 245, 315)$ in $M^3$. Then the inverse image $S$ of $P_1$ in $(\mathbb{Q}^*)^3$ contains all odd multiples of $\bar{P}$, and is infinite by the argument above.
Any point in $S$ has the property that

$$(T - 70, T, T + 70) = (175x_1^2, 245x_2^2, 315x_3^2)$$

for rational numbers $x_1, x_2, x_3$. The result follows as $t = T/35$.

The methods above are all an imitation of [2, p. 252].

By Lemma 1, there are infinitely many rational numbers $t$ such that $(t - 2, t, t + 2) \sim (5, 7, 1)$. These give rise to infinitely many Laguerre polynomials $F_\gamma(x, t) = F_\gamma(x, \lambda, 1), \lambda = t - 4$. The resulting splitting fields over $Q$ cannot be disjoint, since they all contain the discriminant field $Q(\sqrt{3})$. Nevertheless, for all of them the obstruction for $S_7$ vanishes, as we shall now show.

**Lemma 2.** Let $t$ be one of the rational numbers satisfying (3.4), and let $F = F_\gamma(x, t)$. If $F$ is irreducible in $Q[x]$, then $F$ satisfies

$$e = w(2, \Delta) = 1$$

in $Br_2(Q)$, where $w$ is the Witt invariant of the trace form of $Q[x]/(F)$ and $\Delta = \text{discriminant of } F/Q$, considered as an element of $Q^*/Q^{*2}$.

**Proof.** In the notation of [2, p. 254] we have

$$e = (A_2, A_3, A_4, A_5, A_6, A_7)(-1, \prod_{i=1}^{6} A_i)(2, \Delta),$$

where $A_1 \sim 7$ and

$$
\begin{align*}
&c_2 = t - 2 \sim 5 & A_2 \sim 6c_7 \\
&c_3 = t - 1 & A_3 \sim 35c_6 \\
&c_4 = t - 7 & A_4 \sim 6c_5c_7 \\
&c_5 = t + 1 & A_5 \sim 105c_4c_6 \\
&c_6 = t + 2 \sim 1 & A_6 \sim 3c_3c_5c_7 \\
&c_7 = t + 3 & A_7 \sim \Delta \sim 3.
\end{align*}
$$

Substituting and cancelling like terms gives

$$e = (2, 3)(2, 5)(6, 7)(t + 3, 21)(t + 1, 21) \times (t + 1, 5)(t - 1, 5)(t - 1, -1)(t + 3, -1).$$

We can simplify because

$$(t - 1, 5)(t - 1, -1) = (t - 1, -5) = (5u^2 + 1, -5u^2) = 1$$

$$(t + 3, -1) = (v^2 + 1, -1) = 1$$
and so

\[ e = (2, 5)(2, 3)(6, 7)(t + 3, 21)(t + 1, 21)(t + 1, 5). \]

Now

\[
(t + 3, 21) = (7u^2 + 3, 21) = (21u^2 + 9, 21)(3, 21)
= (21u^2 + 9, -21)(21u^2 + 9, -1)(3, 21)
= \left(\frac{21u^2}{9} + 1, -\frac{21u^2}{9}\right)(3, -1)(t + 3, -1)(3, 21)
= (3, -1)(3, 21)(t^2 + 1, -1) = (3, -1)(3, 21) = (3, 7).
\]

As \((2, 7) = 1, (3, 7)(6, 7) = (2, 7) = 1, so now\]

\[ e = (2, 5)(2, 3)(t + 1, 3)(t + 1, 5)(t + 1, 7). \]

But

\[
(t + 1, 7) = (7u^2 + 1, 7) = (7u^2 + 1, -7u^2)(7u^2 + 1, -1)
= (7u^2 + 1, -1) = (t + 1, -1)
\]

so

\[ e = (2, 5)(2, 3)(t + 1, -15). \]

Since \((t + 1, -15) = (5u^2 + 3, -15) = (3, -15)(15u^2 + 9, -15) = (3, 5)\]
\times \(15u^2/9 + 1, -15u^2/9\) = (3, 5), we have finally

\[ e = (2, 3)(2, 5)(3, 5) = (6, 5)(2, 3) = (6, -5)(6, -1)(2, 3)
= (6, -1)(2, 3) = (2, -1)(3, -1)(2, 3) = (3, -2) = 1. \]

We want to show that the infinite set of values \(t\) in (3.4) give rise to infinitely many distinct \(S_7\) (and so \(S_5\)) extensions of \(Q\) which are linearly disjoint over \(Q(\sqrt{3})\). Consider the polynomial \(F_7(x, \lambda, 1)\), where \(\lambda\) is an indeterminate over \(Q\), and set \(t = \lambda + 4\). Let \(F = F_7(x, \lambda, 1) = F(x, t)\), and consider it as a polynomial over \(Q(t)\). The splitting field \(M\) of \(F\) over \(Q(t)\) contains the discriminant field \(E = Q(t)(\sqrt{\Delta})\), \(\Delta = 105(t^3 - 4t)\). Clearly \(G(M/Q(t)) = S_7\); this can be verified by, for instance, the specialization \(t = 7\). Furthermore, \(M\) is a regular extension of \(Q\), as noted before. Similarly, if \(K\) is any number field, then \(MK\) is a regular \(S_7\) extension of \(K(t)\).

Since \(E\) is defined by the equation \(y^2 = 105(t^3 - 4t)\), \(E\) is an elliptic function field, and so has genus 1. As an application of Faltings' theorem \([1]\), we have
LEMMA 3. Let K be a number field. Then

(1) Any subfield N of MK properly containing EK satisfies g(N) > 1, where g(N) is the genus of N over K.

(2) Let $\Delta_0$ be any fixed class in $K^*/K^{*2}$, and denote by $K(\sqrt{\Delta_0})$ the corresponding quadratic extension of K. Let S be a set of rational numbers such that $\Delta$ specializes to $\Delta_0$ for any specialization $t \rightarrow t_0 \in S$. Then for all but finitely many $t_0 \in S$, the Galois group of $F_7(x, t_0)$ over $K(\sqrt{\Delta_0})$ is the alternating group $A_7$.

Proof. For (1), let N be a field, $EK \subset N \subset MK$. Since $g(EK) = 1$, we have $g(N) \geq 1$ by the Riemann–Hurwitz formula, and we must eliminate the possibility $g(N) = 1$. Suppose this were so. Then $N/EK$ is an elliptic covering of an elliptic function field, and [7, Theorem 4.10, p. 76] applies. This says that $N/EK$ must be Galois and abelian corresponding to an abelian homomorphic image of $G(MK/EK)$. But $G(MK/EK)$ is the simple group $A_7$, and so the only possibility is $N = EK$.

For (2), suppose $H$ is a proper subgroup of $A_7$. Suppose $t_0 \in S$ is a value for which $t \rightarrow t_0$ yields Galois group equal to $H$. Set $N = (MK)^H$, the subfield of $MK/EK$ corresponding to $H$. Let $D(x, t) \in K[x, t]$ be a defining equation for $N/K(t)$. By (1), $D(x, t)$ describes a curve of genus larger than 1. Since the specialization $t \rightarrow t_0$ identifies the image of N with the image of E, this specialization must correspond to a rational point $(x_0, t_0)$ to $D(x, t)$ in $K(\sqrt{\Delta_0})$. By Faltings' theorem, there can be only finitely many such rational points for $D(x, t)$ in this number field. Thus the possible set of $t_0$ is finite. As the number of subgroups $H$ is also finite, the result follows.

The argument above is due independently to Serre and Fried, and was communicated to us by W. Feit. An immediate consequence is:

THEOREM 3. There are infinitely many extensions of $Q$ with Galois group $S_7$ which are linearly disjoint over a common discriminant field $Q(\sqrt{3})$.

Proof. Consider the splitting fields of the Laguerre polynomials $F_7(x, t)$, where $t$ is in the infinite set $S$ guaranteed by (3.4) and Lemma 1. By Lemma 3, infinitely many of these $F_7(x, t)$ have Galois group $S_7$ over $Q$ with discriminant field $Q(\sqrt{3})$, and each can be extended to an $S_7$ extension by Lemma 2 and Theorem 1.

We must then settle the issue of the linear disjointness. Any two $S_7$ extensions obtained in this way are identical, or they intersect in either the discriminant field or the field corresponding to $S_7$ (since $S_7$ has a unique composition series). Hence, it is enough to show the $S_7$ extensions give rise to an infinite set of linearly disjoint fields over $Q(\sqrt{3})$.

Suppose, on the contrary, we obtained only finitely many $S_7$ extensions
in this way, and let $K$ be their composite. Of course $\sqrt{3} \in K$, but we can apply Lemma 3 for this field $K$. The conclusion of Lemma 3 says there is an infinite subset $S_1 \subset S$ so that $t_1 \in S_1 \Rightarrow F_1(x, t_1)$ has Galois group $A_t$ over $K$. It follows that for these $t_1$, $F_1(x, t_1)$ has Galois group $S_\gamma$ over $Q$, and the splitting fields are linearly disjoint from $K$ over $Q(\sqrt{3})$. Theorem 3 follows.

**Corollary 1.** Let $K$ be a number field which does not contain $\sqrt{3}$. Then $S_\gamma$ is a Galois group over $K$.

**Proof.** $K$ cannot meet any of the normal fields in Theorem 3 in the discriminant field, since $\sqrt{3}$ is not in $K$. This means that the normal closure of the intersection of any one of them with $K$ either will be $Q$ or will contain the full $S_\gamma$ extension. As these $S_\gamma$ extensions are linearly disjoint over $Q(\sqrt{3})$, we conclude that $K$ cannot meet more than a finite number of the fields in Theorem 3. For any of the rest, the composite with $K$ will have the required property.

**Remark.** If $G$ is a group, we denote by $G^n$ the direct product of $G$ with itself $n$ times. If $G = S_\gamma$, Theorem 3 does not give the conclusion that $G^n$ is a Galois group over $Q$ for all $n$. Using methods that we will expand later in the development of Theorem 4, we have verified by computer search that $G^n$ is a Galois group over $Q$ for $n \leq 14$, but we are not aware of how to prove this for any $n$. The same problem arises for all number fields which do not contain $\sqrt{3}$.

In order to obtain a result like Corollary 1 for fields containing $\sqrt{3}$, we need a new construction. We seek rational numbers $t$ so that

$$(t - 2, t, t + 2) \sim (3, 5, t + 2).$$ (3.5)

Of course $t = 5$ gives an example of (3.5), but we seek infinitely many such rational numbers. Obtaining all such rational numbers $t$ can be obtained by solving the equations

$$t = 5u^2, \quad t - 2 = 3v^2,$$

giving the single Pell equation

$$5u^2 = 3v^2 + 2$$

with rational point $u = v = 1$. The parametric solution of Pell's equation gives: All solutions of (3.5) in rational numbers are of the form

$$t + 2 = \frac{63u^4 - 180u^3 + 270u^2 - 300u + 175}{(3u^2 - 5)^2}$$ (3.6)

as $u$ ranges over all rational numbers.
**Lemma 4.** Let \( F_7(x, t) = F_7(x, \lambda, 1), \ t = \lambda + 4, \) be the Laguerre polynomial of degree 7, where \( t \) satisfies (3.5). Then the obstruction for \( S_7^- \) is

\[
e = (3, 7)(\alpha, 3) = (3, 7\alpha),
\]

where \( \alpha \) is the expression on the right hand side of (3.6).

**Proof.** We set \( y = t + 2 \) where \( t \) is a solution of (3.5). Using the notation of [2, p. 254], we have

\[
c_2 = y - 4, \quad c_3 = y - 3 \sim 3, \quad c_4 = y - 2,
\]

\[
c_5 = y - 1 \sim 5, \quad c_6 = y, \quad c_7 = y + 1
\]

and so

\[
A_1 \sim 7, \quad A_2 \sim 6(y + 1), \quad A_3 \sim 35y,
\]

\[
A_4 \sim 6(y - 1)(y + 1), \quad A_5 \sim 21y,
\]

\[
A_6 \sim 3(y + 1)(y - 1)(y - 3), \quad A_7 \sim 7y.
\]

Then, as on page 254 of [2],

\[
e = (A_2, A_1 A_3)(A_4, A_3 A_5)(A_6, A_5 A_7)(-1, A_1 A_2 \cdots A_6)(2, 7y)
\]

and so

\[
e = (6(y + 1), 5y)(6(y - 1)(y + 1), 15)(3(y - 1)(y + 1), 3)
\times (-1, 35(y + 1)(y - 3))(2, 7y).
\]

We expand this using bilinearity and

\[
(2, 7) = 1
\]

\[
(y + 1, y) = (y + 1, -y)(y + 1, -1) = (y + 1, -1)
\]

\[
(y - 3, -3) = (3u^2 + 1, -3) - (3u^2 + 1, -3u^2) = 1.
\]

The result after simplification is

\[
e = (2, 3)(-1, 7)(y, 3)(y - 1, 5).
\]

Now \((y - 1, 5) = (5u^2 + 1, 5) = (5u^2 + 1, -5u^2)(5u^2 + 1, -1) = (5u^2 + 1, -1)\), and then

\[
(y - 1, 5) = (3v^2 + 3, -1) = (3, -1)(v^2 + 1, -1) = (3, -1) = (2, 3).
\]
Thus

\[ e = (y, 3)(-1, 7). \]

The result follows since \((-1, 7) = (3, 7)\).

**Theorem 4.** Let \( G = S_7 \) and let \( K \) be a number field containing \( \sqrt{3} \). Then there is a Galois regular extension \( M \) of the rational function field \( K(u) \) so that \( G(M/K(t)) \cong G \). In particular, \( G^n \) is a Galois group over \( K \) for all \( n \geq 1 \).

**Proof.** Consider the polynomial \( F = F_3(x, t) \) for \( t \) determined by (3.6). We consider \( F \) as an element of \( Q(u)[x] \). By specializing \( u \) into \( Q \), one can easily show that \( F \) is irreducible with Galois group \( S_7 \); this is easy to verify when \( u = 1 \) by factoring modulo small primes. Let \( M \) be the splitting field of \( F \) over \( K(u) \). \( M \) is regular since the discriminant field is \( E = K(u)(\sqrt{\Delta}), \Delta = 105(t - 2)t(t + 2) \), and this is clearly regular over \( K \). Any algebraic extension of \( K \) in \( M \) must have its normal closure in \( M \), and this would have to contain \( E \).

The obstruction for embedding \( M \) into \( S_7^- \) extension of \( K(t) \) is, by Lemma 4,

\[ e = (3, 7a). \]

As 3 is a square in \( K \), \( e = 1 \), and so \( M \) can be embedded in an \( S_7^- \) extension which is regular over \( K \). The fact that \( G^n \) is then a Galois group over \( K \) follows as a standard application of Hilbert’s irreducibility theorem.

**Theorem 5.** \( S_7^- \) is a Galois group over every number field.

**Proof.** If \( \sqrt{3} \) is not in \( K \), then Corollary 1 applies; otherwise Theorem 4 applies.

4. CENTRAL EXTENSIONS

We consider the question of whether all central extensions of \( S_n \) are Galois groups over \( Q \). The situation for general \( n \) is presently intractable, since it is not currently known whether the groups \( S_n^\pm \) are always Galois groups over \( Q \); the smallest open cases by Theorem A are the groups \( S_{12}^+ \) and \( S_{13}^+ \). We get positive information here for \( n \leq 6 \).

A central extension \( G \) of \( S_n \) is a finite group \( G \) which fits into an exact sequence

\[ 1 \rightarrow A \rightarrow G \rightarrow S_n \rightarrow 1 \]
with $A \subset Z(G) = \text{center of } G$. Let $G' = (G, G)$ denote the commutator subgroup of $G$. If in the sequence above we have also $A \subset G'$, then we say $G$ is a stem extension of $S_n$. Every stem extension is a homomorphic image of a stem cover or Darstellungsgruppe. We have similarly the notions of a stem extension and stem cover of any finite group $H$.

In all that follows, we denote by $C_m$ the cyclic group of order $m$. $|G|$ will denote the order of a finite group $G$. $\tilde{A}_n$ will indicate the group $A_n^{\pm} \cong A_n^-$. We denote by $G''$ the second commutator subgroup of a group $G$. $S_n^{\pm} \times_{C_2} C_{2m}$ will stand for the pullback of $S_n$ and $C_{2m}$ along the canonical projections

$$S_n^{\pm} \to C_2 \leftarrow C_{2m}.$$  

Our next theorem reduces the problem of central extensions to these pullbacks:

**Theorem 6.** Fix an integer $n \geq 2$. If $k$ is a number field and $S_n^{\pm} \times_{C_2} C_{2m}$ are Galois groups over $k$ for all $m > 1$, then every finite central extension of $S_n$ is a Galois group over $k$.

**Proof:** Let

$$1 \to A \to G \to S_n \to 1$$

be a central extension, with $A$ finite and contained in $Z(G)$. We suppose that $G$ is a minimal counterexample to Theorem 6. Let $U$ be a minimal cover of $S_n$ in $G$; i.e., $U$ is a subgroup of $G$ such that $UA = G$ and $VA \neq G$ for any proper subgroup $V$ of $U$. Then $UA = G$ is a homomorphic image of the direct product $U \times A$ under the map $(u, a) \to ua$, $u \in U$, $a \in A$. If $U$ is a Galois group over $k$, say $U = G(K/k)$, then taking an extension $L/k$ with $G(L/k) \cong A$ and $L \cap K = k$, we conclude that $U \times A$ is a Galois group over $k$, hence $UA = G$ is also. Clearly $U$ is a central extension of $S_n$, and so by minimality we may assume that $U = G$. Thus we may assume that $G$ is an essential extension of $A$; i.e., $UA = G \Rightarrow U = G$ for subgroups $U$ of $G$.

The commutator subgroup $G'$ must map onto the commutator subgroup $S_n' = A_n$ of $S_n$, and so $G/A \cong S_n \Rightarrow (G/A)' = G'A/A \cong A_n$. Furthermore, since $A_n' = A_n$, we have $(G'A/A)' = G''A/A \cong G'A/A$, and so

$$G''A = G'A. \quad (4.1)$$

Now let $\sigma$ be an element of $G$ such that $\sigma \mod A$ is a transposition. Then $\sigma^2 \in A$, and replacing $\sigma$ by an odd power if necessary, we may suppose that $\sigma$ has 2-power order.

Denote by $(A, B)$ the subgroup generated by all commutators $aba^{-1}b^{-1}$, $a \in A$, $b \in B$. Then $(G, G') = (G, G'A)$ since $A \subset Z(G)$, and so

$$(G, G') = (G, G'A) = (G, G''A) = (G, G'') \subset G''$$
since $G'' \triangleleft G$. This gives

$$G'/G'' \subset Z(G/G'').$$ (4.2)

Also since $\langle \sigma \rangle G' A = G$, $U = \langle \sigma \rangle G'$ is a cover in the sense that $UA = G$. Because $G$ is now an essential extension, we have

$$\langle \sigma \rangle G' = G.$$ (4.3)

Thus $G/G' = \langle \sigma \rangle G'/G'$ is cyclic. By (4.2), $G/G''$ modulo its center is also cyclic. A standard exercise shows that if a group modulo its center is cyclic, the group must be abelian. Hence $G/G''$ is abelian, which implies

$$G'' = G'.$$

This means that $G'$ is a stem extension of $A_n$ by $G' \cap A$. Since $A_n$ has the unique stem cover $\tilde{A}_n$, we see that $G' \cong A_n$ or $\tilde{A}_n$.

By (4.3), $G = \langle \sigma \rangle G'$, so $G$ is a homomorphic image of the semidirect product $\langle \sigma \rangle \rtimes G'$ under the map $(\sigma^i, g) \mapsto \sigma^i g$. Thus it suffices to realize $\langle \sigma \rangle \rtimes G'$ as a Galois group over $k$. In order to avoid confusion, let $\langle \sigma_1 \rangle$ and $G_1$ be isomorphic copies of $\langle \sigma \rangle$ and $G$ respectively, where $\sigma_1$ acts on $G_1$ by conjugation the way $\sigma$ acts on $G$.

**Claim.**

$$\langle \sigma_1 \rangle \rtimes G_1 \cong \begin{cases} S_n \times C_2^m & \text{for some } m \text{ if } G' \cong A_n \\ S_n^\pm \times C_2^m & \text{for some } m \text{ if } G' \cong \tilde{A}_n. \end{cases}$$

**Proof.** Let $M = \langle \sigma_1 \rangle \rtimes G_1$, $N$ the subgroup $\langle \sigma_1^2 \rangle \cdot G'_1$ of $M$. Since $\sigma^2 \in Z(G)$, $\sigma_1^2$ acts trivially on $G_1$, so $N = \langle \sigma_1^2 \rangle \cdot G'_1$ is a direct product. The epimorphism $M \to G$ maps $M/\langle \sigma_1^2 \rangle$ onto $G/\langle \sigma^2 \rangle$, which in turn maps canonically onto $G/A \cong S_n$. Also $|M/\langle \sigma_1^2 \rangle| = 2|G'|$.

If $G' \cong A_n$, then $|M/\langle \sigma_1^2 \rangle| = |S_n|$, and so $M/\langle \sigma_1^2 \rangle \cong S_n$. If $G' \cong \tilde{A}_n$, then $M/\langle \sigma_1^2 \rangle$ is a central extension of $S_n$ by $C_2$ and contains $\tilde{A}_n$. Therefore $M/\langle \sigma_1^2 \rangle \cong S_n^\pm$. We set $D = M/\langle \sigma_1^2 \rangle$ (which is $S_n$ or $S_n^\pm$), and $E = M/G'_1 \cong \langle \sigma_1^2 \rangle \cong C_2^m$. Also $C_2 \cong M/N$. The claim follows from the commutative diagram

$$
\begin{array}{ccc}
M & \longrightarrow & E \\
\downarrow & & \downarrow \\
D & \longrightarrow & C_2.
\end{array}
$$

This completes the proof of Theorem 6.
For $n \leq 4$ all central extensions of $S_n$ are solvable groups, and so are Galois groups over $Q$ by the well known theorem of Safarevic. We consider the cases $n = 5$ and $n = 6$. In Galois theory terms, Theorem 6 translates to the following: to find an $S_n^+$ and $S_n^-$ extension of $Q$ so that the discriminant subfield of the $S_n$ extension can be extended to a cyclic group of order $2^m$. We make another reduction in order to accomplish this:

**Theorem 7.** Let $f(x) \in Q[x]$ be a polynomial of degree $n$ whose normal closure $M$ satisfies:

1. $G(M/Q) \cong S_n$
2. The discriminant subfield of $M$ is $Q(\sqrt{2})$
3. $M$ can be extended to an $S_n^+$ or $S_n^-$ extension of $Q$.

Then all central extensions of $S_n$ are Galois groups over $Q$.

**Proof.** When $\Delta \sim 2$, then the obstructions for $S_n^+$ and $S_n^-$ are actually identical, since we have by Theorem 1

$$e(S_n^+) = w(2, 2)$$
$$e(S_n^-) = w(-2, 2).$$

As $(2, 2) = (-2, 2) = 1$, both obstructions above reduce to the Witt invariant $w$. The field $Q(\sqrt{2})$ is the unique quadratic extension of $Q$ which can be extended to a cyclic extension of degree $2^m$ for all $m \geq 2$. Thus $S_n^+ \times C_2 \times C_{2m}$ and $S_n^- \times C_2 \times C_{2m}$ would be Galois groups over $Q$ by taking composites of $M$ with the extending $C_{2m}$ extensions. Theorem 6 then guarantees all central extensions of $S_n$ would be Galois groups over $Q$.

**Theorem 8.** Every central extension of $S_n$ is a Galois group over $Q$ for $n \leq 6$.

**Proof.** We construct the polynomials of degree 5 and 6 required in Theorem 7.

*The case $n = 5*. We follow the development of Lemma 3-5 and Theorem 2 of [8]. We set

$$m = 2, \quad a = \frac{271}{6}, \quad b = 30, \quad c = -\frac{269}{6}$$

in the context of [8]. Then

$$\lambda = 2b^2 - 15ma^2 = -\frac{356405}{6}, \quad \mu = \frac{30a^2 - b^2}{2} = \frac{361805}{12}$$
in the set-up of [8]. The development in [8] shows that $F_5(x, \lambda, \mu)$ is irreducible over $\mathbb{Q}$ with Galois group $S_5$, discriminant field $\mathbb{Q}(\sqrt{2})$, and the obstruction for $S_5^+$ vanishes. One can find integral values of $\lambda$ and $\mu$ by rescaling (since only $\lambda/\mu$ is relevant): $\mu = 361805, \lambda = -712810$.

The case $n = 6$. Consider the Laguerre polynomial $f = F_6(x, \lambda, 1)$ with $\lambda = 4$. Then the formulas in [2, p. 237] show that the discriminant is

$$d = 15 \cdot 6 \cdot 8 \cdot 10 \sim 2.$$ 

An easy calculation (which we did by computer) shows that $f$ is irreducible (mod 11), has irreducible factors of degrees 1 and 5 (mod 17), and has irreducible factors of degrees 1, 2, and 3 (mod 19). This means the Galois group contains 6-cycles, 5-cycles, and transpositions, and so must be $S_6$. Using [2, Theorems 3.1 and 5.1], it is easy to show that the obstruction for $S_6^+$ vanishes, so $f$ will serve by Theorem 7. This completes the proof of Theorem 8.

ACKNOWLEDGMENT

During the course of this work, Murray Schacher was a Fulbright Fellow at the Catholic University of Louvain in Louvain-la-Neuve, Belgium. He thanks the Institute of Nuclear Physics at that university for the generous use of its computer facilities, which were especially useful for computations of Galois groups of explicit polynomials.

REFERENCES

2. W. Feit, $\widetilde{A}_5$ and $\widetilde{A}_7$ are Galois groups over number fields, J. Algebra 104, 2 (1986), 231–260.
4. M. Schacher and J. Sonn, Double covers of the symmetric groups as Galois groups over number fields, J. Algebra, in press.
8. J. Sonn, Double Covers of $S_5$ and Frobenius groups as Galois groups over number fields, J. Algebra, in press.