Double Covers of $S_5$ and Frobenius Groups as Galois Groups over Number Fields

JACK SONN

Department of Mathematics, Technion, Haifa 32000, Israel

Communicated by Walter Feit

Received August 1, 1986

It is proved that the two double covers of $S_5$ are Galois groups over every number field. This, together with same result for the double cover of $A_5$, proved by Feit, yields the result that every Frobenius group is a Galois group over every number field.

INTRODUCTION

In this paper we prove that the double covers $S_n^+$ and $S_n^-$ of the symmetric group $S_5$ are realizable as Galois groups over any number field (finite over $Q$). Recently Feit [3] has proved the same for $A_n^+ \simeq SL(2, 5)$.

As a result of [1, 2, 7], we thus have:

THEOREM. Every Frobenius group is realizable as a Galois group over every number field.

A Frobenius group is a finite transitive permutation group in which every element different from 1 has at most one fixed point. The above theorem was proved for $Q$ in [12], by finding a particular polynomial for $S_5$ (resp. $A_5$) whose splitting field is embeddable into an $S_5^+$ (resp. $A_5^+$) extension. The polynomial for $A_5$ was a generalized Laguerre polynomial; Galois groups of such polynomials were originally computed by Schur [9]. More recently, Serre [10] proved a theorem relating the obstruction to embedding problems of the above type to the Witt invariant of the trace form. Vila [14] has applied this to realizing $A_n^+$ over $Q(t)$ for most $n \equiv 0, 1, 2, 3$ (mod 8), and Feit [3] has computed the Witt invariant of generalized Laguerre polynomials, realizing $A_n^+$ and $A_n^-$ over every number field, as well as $A_n^+$ over $Q$ for $n \equiv 3(4)$. Indeed Feit proves that the same fields constructed by Schur for $A_n$ are embeddable into $A_n^+$ extensions for $n \equiv 3(4)$.
Our method of proof is to use Serre's formula and a modification of it in conjunction with results and ideas from [3] to produce infinitely many linearly disjoint $S_3$ (resp. $S_3'$) extensions of $\mathbb{Q}$.

1. SERRE'S FORMULA

Let $Q$ be a nondegenerate quadratic form in $n$ variables over a field $K$ of characteristic $\neq 2$. If for $a, b \in K^*$, $\{a, b\}$ denotes the generalized quaternion algebra generated by $u, v$ over $K$, satisfying $u^2 = a, v^2 = b, vu = -uv$, and $(a, b)$ its class in the Brauer group $Br(K)$, then the Witt invariant $w_2(Q)$ of $Q$ is defined by

$$w_2(Q) = \prod_{i < j} (a_i, a_j),$$

where

$$Q \sim a_1 X_1^2 + \cdots + a_n X_n^2.$$

If $G_K$ denotes the absolute Galois group of $K$, then the subgroup $Br_2(K)$ of $Br(K)$ consisting of elements killed by 2 can be identified with $H^2(G_K, \mathbb{Z}/2\mathbb{Z}) = H^2(G_K)$. Observe that $w_2(Q) \in Br_2(K)$. Furthermore, $H^1(G_K, \mathbb{Z}/2\mathbb{Z}) = H^1(G_K)$ can be identified with $K^*/K^{*2}$, and with the above identifications, the symbol $(, )$ coincides with the cup product

$$H^1(G_K) \times H^1(G_K) \rightarrow H^2(G_K).$$

(For details on this section see [10].)

The first and second cohomology groups $H^i(S_n) = H^i(S_n, \mathbb{Z}/2\mathbb{Z})$ of the symmetric groups $S_n$ are well known:

$$H^1(S_n) = \begin{cases} 0 & n = 1 \\ \mathbb{Z}/2\mathbb{Z} & n \geq 2 \end{cases}$$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & n = 2, 3 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & n \geq 4 \end{cases}$$

The nonzero element of $H^2(S_n)$ for $n \geq 2$ is the parity function

$$\varepsilon_n: S_n \rightarrow \{ \pm 1 \} \cong \mathbb{Z}/2\mathbb{Z}.$$
(1) \( S_n \times C_2 \).

(2) \( S_n \times C_4 \), the pullback of \( S_n \to C^2 \leftrightarrow C_4 \). This element can also be identified with \( e_n \cdot e_n \), where \( \cdot \) denotes the cup product.

For \( n \geq 4 \) we have the two additional extensions:

(3) \( S_n^+ \), with corresponding \( s_n^+ \in H^2(S_n) \).

(4) \( S_n^- \), with corresponding \( s_n^- \in H^2(S_n) \).

In Serre [10] \( s_n^- \) is denoted by \( s_n \). In Schur [8, p. 355] \( S_n^+ \), \( S_n^- \) are denoted \( (T_n) \) and \( (T_n') \), respectively.

\( S_n \) has a standard presentation with generators \( t_1, \ldots, t_{n-1} \) (\( t_i \) is the transposition \( (i, i + 1) \)) and relations

\[
\begin{align*}
t_i^2 &= 1, & i &= 1, \ldots, n-1, \\
(t_it_{i+1})^3 &= 1, & i &= 1, \ldots, n-2, \\
t_i &= t_{i+j}, & i &= 1, \ldots, n-2, j \geq i+2.
\end{align*}
\]

There correspond presentations of \( S_n^+ \):

- generators \( a, x_1, \ldots, x_{n-1} \), with relations \( a^2 = 1, x_i^2 = a \) (\( 1 \leq i \leq n-1 \)), \( (x_ix_{i+1})^3 = a \) (\( 1 \leq i \leq n-2 \)), \( x_ix_j = ax_jx_i \) (\( i = 1, \ldots, n-2, j \geq i+2 \));

and of \( S_n^- \):

- generators \( b, y_1, \ldots, y_{n-1} \), with relations \( b^2 = 1, y_i^2 = 1 \) (\( 1 \leq i \leq n-1 \)), \( (y_iy_{i+1})^3 = 1 \) (\( i = 1, \ldots, n-2 \)), \( by_i = y_ib \) (\( 1 \leq i \leq n-1 \)), \( y_iy_j = by_jy_i \) (\( i = 1, \ldots, n-2, j \geq i+2 \)).

Let \( e: G_K \to S_n \) be a continuous homomorphism, \( e^*: H^2(S_n) \to H^2(G_K) = Br_2(K) \) the induced map.

Now let \( f(x) \in K[x] \) be a separable irreducible polynomial of degree \( n \), \( E = K[x]/(f(x)) \), \( Q_E(x) = \text{tr}(X^2) \), \( X \in E \), the trace quadratic form on \( E \).

Let \( d_E \in K^*/K^{*2} \in H^1(G_K) \) be the discriminant of \( E \). Let \( L \supseteq E \) be the splitting field of \( f(x) \), \( G = G(L/K) \), \( e: G_K \to G(L/K) \subseteq S_n \) the restriction map.

**Theorem 1** (Serre’s formula [10, p. 655]). \( w_2(Q_E) = e^*(s_n^-) + (2, d_E) \) (written additively).

**Corollary.** \( w_2(Q_E) = e^*(s_n^+) + (-2, d_E) \).

---

1 W. Feit has informed me that he and Serre independently have also proved this corollary.
Proof. Since in $H^2(S_5)$, $s_n^+ = (\varepsilon_n \cdot \varepsilon_n) + s_n^-$, we have $e^*(s_n^+) = e^*(\varepsilon_n \cdot \varepsilon_n) + e^*(s_n^-)$. By the commutativity of the diagram

$$H^1(G_K) \times H^1(G_K) \to H^2(G_K)$$

we have $e^*(\varepsilon_n \cdot \varepsilon_n) = e^*(\varepsilon_n) \cdot e^*(\varepsilon_n)$. By Kummer theory, it is easy to see that $e^*(\varepsilon_n) = d_E$. Thus $e^*(s_n^+) = (d_E, d_E) + e^*(s_n^-)$. But $(d_E, d_E) = (-1, d_E) + (-d_E, d) = (-1, d_E)$. By Serre's formula, $e^*(s_n^-) = w_2(Q_E) + (2, d_E)$; hence $e^*(s_n^+) = (-1, d_E) + w_2(Q_E) + (2, d_E) = (-2, d_E) + w_2(Q_E)$. 1

Let $1 \to A \to H \to G \to 1$ be a group extension, $A$ abelian, $H$ finite. If $e: G_K \to G$ is a continuous epimorphism, it is well known [6] that if $e \in H^2(G, A)$ is the cohomology class corresponding to the given group extension, then $e^*(c) = 0$ if and only if $e$ can be lifted to a (continuous) homomorphism $g: G_K \to H$ s.t. $f \circ g = e$. Thus Serre remarks that in the case $A = \mathbb{Z}/2\mathbb{Z}$, the obstruction $e^*(s_n^-)$ can be computed by the formula

$$e^*(s_n^-) = w_2(Q_E) + (2, d_E)$$

provided, of course, one can compute the right-hand side. Similarly,

$$e^*(s_n^+) = w_2(Q_E) + (-2, d_E).$$

In addition, if $G \subseteq A_n$ (alternating group), then $(2, d_E) = 0$, so

$$e^*(a_n) = w_2(Q_E),$$

where $a_n$ is the restriction of $s_n^-$ (and of $s_n^+$) to $A_n$. This is the form of Serre's formula used by Vila and Feit.

Because of its importance to Frobenius groups, we are particularly interested in $s_5^+$, however, since our method applied also to $s_5^-$, we deal with both $S_5^+$ and $S_5^-$. In what follows we will need the local decomposition of $Br(Q)$; i.e., the fundamental exact sequence [7, p. 277]

$$0 \to Br(Q) \to \bigoplus_p Br(Q_p) \to Q/Z \to 0.$$
where \( p \) runs through all the rational primes including \( \infty \). From this we have the exact sequence

\[
0 \to \text{Br}_2(\mathbb{Q}) \to \bigoplus_p \text{Br}_2(\mathbb{Q}_p) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to 0
\]

\[
e \to (c_p) \quad (c \in \text{Br}(\mathbb{Q}))
\]

\[
(a, b) \to ((a, b)_p) \quad (a, b \in \mathbb{Q}^*)
\]

Here \( (a, b)_p \) can be identified with the local quadratic norm residue symbol.

2. The Construction

Given \( \lambda, \mu \) indeterminates, the corresponding (normalized) generalized Laguerre polynomial of degree \( n \) is given by

\[
F_n(x, \lambda, \mu) = x^n - nc_n x^{n-1} + \binom{n}{2} c_n c_{n-1} x^{n-2} - \cdots + (-1)^n c_n c_{n-1} \cdots c_1,
\]

where \( c_i = \lambda + i\mu \) \([9, 12, 3]\). Its discriminant is

\[
D_n(\lambda, \mu) = n! \mu^{(n(n-1)/2)} \prod_{i=1}^{n} (ic_i)^{i-1}.
\]

Write \( a \sim b \) if \( ab^{-1} \) is a square in \( \mathbb{Q}(\lambda, \mu) \). Then

\[
D_5(\lambda, \mu) \sim 15c_2 c_4.
\]

Let \( \lambda, \mu \in \mathbb{Q}^* \), \( D_5(\lambda, \mu) \neq 0 \), \( E = \mathbb{Q}[x]/(F_5(x, \lambda, \mu)) \), and \( w = w(\lambda, \mu) = w_2(Q_E) \), the Witt invariant.

**Lemma 2 (Feit \([3]\)).** For all \( p \),

\[
w(\lambda, \mu)_p = (3\mu c_4, \mu c_5)_p (\mu c_2, 2c_3 c_5)_p (-1, 6c_3 c_4)_p
\]

or equivalently,

\[
w(\lambda, \mu) = (3\mu c_4, \mu c_5)(\mu c_2, 2c_3 c_5)(-1, 6c_3 c_4).
\]
Let $a, b, m$ be nonzero rational numbers, $m > 0$ such that $15m$ is not a square, $15ma^2 - b^2 > 0$. Set $\lambda = 2b^2 - 15ma^2$, $2\mu = 15ma^2 - b^2$. Then

\[ c_2 = \lambda + 2\mu = b^2 \sim 1 \]
\[ c_3 = \frac{15ma^2 + b^2}{2} = b^2 + \mu \]
\[ c_4 = 15ma^2 \sim 15m \]
\[ c_5 = \frac{45ma^2 - b^2}{2} = 15ma^2 + \mu \]
\[ D = D_5(\lambda, \mu) \sim 15c_2c_4 \sim m. \]

**Lemma 3.** With the above choices of $\lambda, \mu$,
\[ w = (-1, -2)(-6, b^2 - 15ma^2)(-1, m) = (-1, -2)(-6, -2\mu)(-1, m). \]

**Proof.** By Lemma 2,
\[ w = (3mc_4, mc_5)(mc_2, 2c_3c_5)(-1, 6c_3c_4) \]
\[ = (5\mu, mc_5)(\mu, 2c_3c_5)(-1, 6c_3c_4) \]
\[ = (-5\mu, mc_5)(-\mu, mc_5)(-1, 10mc_3)(\mu, 2c_3c_5) \]
\[ = (-5, \mu)(-5, c_5)(m, \mu)(m, c_5)(-\mu, c_5) \]
\[ \times (-1, 2)(-1, 5)(-1, m)(-1, c_3)(\mu, 2)(\mu, c_3)(\mu, c_5) \]
\[ = (-10\mu, 5m, c_3)(-\mu, c_3)(-1, m). \]

Now
\[ (5m, c_3) = (5m, \frac{1}{2}(45ma^2 - b^2)) = (5m, 2(45ma^2 - b^2)) \]
\[ = (5m, -2)(5m, b^2 - 45ma^2) = (5m, -2)(45ma^2, b^2 - 45ma^2) \]
\[ = (5m, -2)\left(\frac{45ma^2}{b^2}, 1 - \frac{45ma^2}{b^2}\right) = (5m, -2). \]

Similarly, $(-10m, \mu) = (-10m, -2)(-6, b^2 - 15ma^2)$.
\[ (-\mu, c_3) = (-\mu, \mu + b^2) = (-\mu, \mu(1 + b^2/\mu)) \]
\[ = (-\mu, 1 + b^2/\mu) = \left(-\frac{b^2}{\mu}, 1 - \left(-\frac{b^2}{\mu}\right)\right) = 1. \]
Thus
\[ w = (5m, -2)(-10m, -2)(-6, b^2 - 15ma^2)(-1, m) \]
\[ = (-1, -2)(-6, b^2 - 15ma^2)(-1, m). \]

**Corollary.**
\[ e^*(s^+_z) = w(-2, m) = (-1, -2)(-6, b^2 - 15ma^2)(2, m) \]
\[ e^*(s^-_z) = (-1, -2)(-6, b^2 - 15ma^2)(-2, m). \]

Note \( e^*(s^+_z)_+ = e^*(s^-_z)_- = 1. \)

By the product formula, if \( e^*(s^+_z)_p \) (resp. \( e^*(s^-_z)_p \)) = 1 for all odd primes \( p \), then \( e^*(s^+_z) \) (resp. \( e^*(s^-_z) \)) = 1. At \( p \) odd, \( (-1, -2)_p = 1 \), hence for \( p \) odd,
\[ e^*(s^+_z)_p = (-6, b^2 - 15ma^2)_p(2, m)_p \]
\[ e^*(s^-_z)_p = (-6, b^2 - 15ma^2)_p(-2, m)_p. \]

**Lemma 4.** Suppose \( a, b \) also satisfy
\[ b^2 - 15ma^2 = -15mc^2 \]
for some nonzero rational number \( c \). Then
\[ e^*(s^+_z)_p = \begin{cases} (-3, m)_p, & p > 3 \\ (-3, m)_p, & p = 3 \end{cases} \]
\[ e^*(s^-_z)_p = \begin{cases} (3, m)_p, & p > 3 \\ (-3, m)_p, & p = 3 \end{cases}. \]

**Proof.** Substituting in the preceding corollary, we get
\[ e^*(s^+_z)_p = (-1, -2)_p(-6, -15m)_p(2, m)_p \]
\[ = (-6, -15)_p(-3, m)_p, \]
\[ e^*(s^-_z)_p = (-6, -15)_p(3, m)_p \]
and note that
\[ (-6, -15)_p = \begin{cases} 1, & p > 3 \\ -1, & p = 3 \end{cases}. \]
Theorem 2. Let \( m = 6q \), where \( q \) is a prime larger than 3, \( q \equiv 1 \pmod{3} \). Set

\[
2a = q + 90, \quad 2c = q - 90
\]

so

\[
a^2 - c^2 = (a + c)(a - c) = 90q = 15m.
\]

Then

\[
a^2 - 15m = c^2,
\]

\[
15ma^2 - (15m)^2 = 15mc^2.
\]

Let \( b = 15m, \ 2\mu = 15ma^2 - b^2 = 15mc^2, \ \lambda = 2b^2 - 15ma^2 \). Then \( F_s(x, \lambda, \mu) \) has Galois group \( S_5 \) and \( e^*(s^+_s) = 1 \), so that the splitting field \( K \) of \( F_s(x, \lambda, \mu) \) over \( \mathbb{Q} \) can be embedded into an \( S_5 \) extension of \( \mathbb{Q} \).

Proof. By the corollary to Lemma 3, \( e^*(s_s^+) \equiv 1 \). By the product formula, \( e^*(s_s^+) = 1 \) if \( e^*(s_s^+) = 1 \) for all odd primes \( p \). By Lemma 4,

\[
e^*(s_s^+) = -(3, 6q) = -(3, 2q),
\]

\[
= - (3, 2q)_3 = - \left( \frac{2q}{3} \right) = - \left( \frac{2}{3} \right) \left( \frac{q}{3} \right) = - (-1) \cdot 1 = 1.
\]

For \( p \neq 3 \), \( e^*(s_s^+) = -(3, 6q)_p = 1 \) if \( p \neq q \), and \( e^*(s_s^+) = -(3, 6q)_q = (3, q)_q = (\frac{-1}{q}) = (\frac{1}{q}) = (-1)^{\frac{q-1}{2}} \frac{1}{2} = 1 \). It remains to prove that the Galois group is \( S_5 \). Writing \( F_s(x, \lambda, \mu) \) out explicitly, we have

\[
F_s(x, \lambda, \mu) = x^5 - 5c_5x^4 + 10c_5c_4x^3 - 10c_5c_4c_3x^2
+ 5c_5c_4c_3c_2x - c_5c_4c_3c_2c_1,
\]

where

\[
c_1 = c_2 - \mu = (15m)^2 - \frac{15mc^2}{2} = \frac{15m}{2} (30m - c^2)
\]
\[
c_2 = b_2 = (15m)^2
\]
\[
c_3 = c_2 + \mu = \frac{15m}{2} (30m + c^2)
\]
\[
c_4 = c_2 + 2\mu = 15m(15m + c^2)
\]
\[
c_5 = c_2 + 3\mu = \frac{45m}{2} (10m + c^2).
\]
We plot the Newton polygons at \( p = 3 \) and \( 5 \); according to the table

<table>
<thead>
<tr>
<th>( i )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{ord}_3(c_i) )</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>( \text{ord}_5(c_i) )</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

at \( p = 3 \), the Newton polygon consists of the two segments from \((0, 13)\) to \((2, 7)\) and from \((2, 7)\) to \((5, 0)\), the latter having slope \(-\frac{3}{5}\). This shows that 3 divides the order of the Galois group.

At \( p = 5 \), we get the single segment from \((0, 6)\) to \((5, 0)\) with slope \(-\frac{2}{5}\), so 5 divides the order of the Galois group.

Since in addition, the discriminant of the polynomial is \( m \mod \text{squares} \), the Galois group is not a subgroup of \( A_5 \). It follows that the Galois group is all of \( S_5 \).

**Theorem 3.** Let \( m = 3q \) where \( q \) is a prime \( \equiv 1 \pmod{12} \). Set

\[
2a = q + 45, \quad 2c = q - 45, \\
b = 15m = 45q, \\
\lambda = 2b^2 - 15ma^2, \quad 2\mu = 15ma^2 - b^2.
\]

Then \( F_5(x, \lambda, \mu) \) has Galois group \( S_5 \) and \( e^*(s_5^{-}) = 1 \), so that the splitting field \( K \) of \( F_5(x, \lambda, \mu) \) can be embedded into an \( S_5^{-} \) extension of \( Q \).

**Proof.** As in Theorem 2, \( e^*(s_5^{-})_x = 1 \), and we are reduced to computing \( e^*(s_5^{-})_p \) at \( p = 3 \) and \( q \). By Lemma 4,

\[
e^*(s_5^{-})_3 = -(3, m)_3 = -(3, 3q)_3 = -(3, -q)_3 \\
= -(3, -1)_3 (3, q)_3 = - \left( \frac{1}{3} \right) \left( \frac{q}{3} \right) = -(-1) \cdot 1 = 1;
\]

\[
e^*(s_5^{-})_q = (3, m)_q = (3, -q)_q = (3, q)_q = \left( \frac{3}{q} \right)
\]

\[= \left( \frac{q}{3} \right) (-1)^{q - 1/2} = 1 \cdot 1.
\]

The Newton polygons at \( p = 3 \) and \( 5 \) are the same as in Theorem 2, hence the Galois group is \( S_5 \).

**Theorem 4.** Let \( E/Q \) be any finite extension. Then there exists a Galois extension \( K/Q \) with \( G(K/Q) \approx S_5^+ \) such that \( E \cap K = Q \). The same holds for \( S_5^- \).
**Proof.** By Dirichlet's density theorem, there are infinitely many $q$ for Theorem 2 and Theorem 3. Let $E$ be given, and choose $q$ unramified in $E$. If $K \cap E \neq \mathbb{Q}$, then $K \cap (\text{normal closure of } E/\mathbb{Q})$ contains the unique quadratic subfield $\mathbb{Q}(\sqrt{m})$ of $K$ ($S_5^+$ (resp. $S_5^-$) has a unique composition series). $q$ is ramified in $\mathbb{Q}(\sqrt{m})$ and unramified in the normal closure of $E/\mathbb{Q}$, contradiction.

**Corollary.** $S_5^+$ and $S_5^-$ are Galois groups over every number field. Similarly, groups such as $S_5^+ \times \cdots \times S_5^+ \times S_5^- \times \cdots \times S_5^-$ are Galois groups over every number field.

**Proof.** Clear.

**Theorem 5.** Every Frobenius group is a Galois group over every number field.

**Proof.** Let $k$ be a number field. Then $A_5^+ \simeq SL_2(5)$ is a Galois group over $k$ by Feit's Theorem [3] and $S_5^-$ is a Galois group over $k$ by the corollary to Theorem 4 above. The result now follows from [11, Theorem 2.7].

**References**

1. E. Abboud, Q-admissibility of $S_5^-$, Israel J. Math., in press.
3. W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields, preprint.
13. L. Stern, Q-admissibility of Sylow metacyclic groups having $S_5^+$ as quotient group, Comm. Algebra, in press.