A new formulation of Netto's argument and the case of degree seven.

Matthew Ingle

We are interested in groups with the following properties:
Let $n \geq 7$ be an odd integer, and consider subgroups $G \leq S_n$ that satisfy:

1. $G = \langle s_1, s_2, s_3, s_4 \rangle$ where $s_1 s_2 s_3 s_4 = 1$.

2. $(s_1, s_2, s_3, s_4) = ((2)^m, (2)^m, (2)^m, (2)^{m-3}(4))$ where $m = \frac{n-1}{2}$. The notation $(2)^m$ means that s_i is a product of m disjoint 2-cycles, and similarly, the cycle decomposition of s_4 consists of $m-3$ disjoint 2-cycles and one 4-cycle.

3. G acts primitively on $S = \{x_1, x_2, ..., x_n\}$.

Such groups occur in [1], pg. 17 (specifically, Prop. 3.6) as the monodromy groups of certain curve covers. In this paper, we prove the following fact about these groups:

Theorem 1. *If a group G satisfies the above conditions then $G = A_n$, if $n \equiv 1 \pmod 4$ and $G = S_n$, if $n \equiv 3 \pmod 4$.*

In our demonstration, the case $n = 7$ will be considered separately because for the case $n \geq 9$ we prove a more general result:

Theorem 2. *If G is a primitive permutation group of degree $n \geq 9$ and G contains a 4-cycle or a $(2,2)$-cycle then $G \geq A_n$.*

The motivation for Theorem 2 came from Netto who, in his *Theory of Substitutions*, gave a sketched proof of an equivalent theorem (cf. [2] pg. 133-8). Unfortunately, a new formulation of his argument was necessary because of some ambiguity in his exposition (see Remark 1 below). In our new formulation, Theorem 2 follows from Propositions 1 and 2 appearing below.

Because it is a more general result, we begin with our proof of Theorem 2 and its antecedent propositions. Following this, we consider the case of $n = 7$ and conclude with our proof of Theorem 1. Before beginning, we need to establish the following terminology:

Definition. Let G be a group acting on a set Ω, and let T be a subset of G. We define the *support* of T by

$$\mathrm{supp}(T) := \{x \in \Omega \mid x^g \neq x \text{ for at least one } g \in T\}.$$

When T is a singleton, i.e. $T = \{g\}$, we write $\mathrm{supp}(g)$ instead of $\mathrm{supp}(\{g\})$. Additionally, due to its ubiquitous application, we define the following shorthand:

$$\mathrm{supp}(g)(h) := \mathrm{supp}(g) \cap \mathrm{supp}(h).$$

Proposition 1. *Let G be a primitive permutation group of degree $n \geq 9$ and let $g_i = a_i b_i \in G$ be two $(2,2)$ cycles such that:*

$$\#\mathrm{supp}(a_1)(a_2) = 1. \tag{1}$$

Then $G \geq A_n$ unless we have:

$$\#\mathrm{supp}(b_1)(a_2) = 0, \#\mathrm{supp}(a_1)(b_2) = 0, \text{ and } \#\mathrm{supp}(b_1)(b_2) = 1. \tag{2}$$

Proof. Let G be a primitive permutation group acting on the set $\Omega := \{1, 2, .., n\}$ with $n \geq 9$ and let $g_i = a_i b_i \in G$ be two $(2,2)$ cycles such that condition (1) holds.

Our argument concerns the following variables: $\#\mathrm{supp}(b_1)(a_2) \in \{0,1\}$, and $\#\mathrm{supp}(b_2)(a_1 b_1) \in \{0,1,2\}$. We begin by supposing that $\#\mathrm{supp}(b_1)(a_2) = 1$, and show that for each possible value of $\#\mathrm{supp}(b_2)(a_1 b_1)$, $G \geq A_n$. Then, we suppose that $\#\mathrm{supp}(b_1)(a_2) = 0$ and show that $G \geq A_n$ unless condition (2) holds.

Claim 1: $\#\mathrm{supp}(b_1)(a_2) = 1 \implies G \geq A_n$.

The following three subcases are organized according to the value of $\#\mathrm{supp}(b_2)(a_1 b_1) \in \{0, 1, 2\}$ wherein we show that in each case, $G \geq A_n$.

Case 0: $\#\mathrm{supp}(b_2)(a_1 b_1) = 0$. Up to conjugacy, we have $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (13)(56)$. Thus, we have $g_3 := g_2 g_1 g_2 = (14)(23) \in G$ and consequently $g_1 g_3 = (13)(24) \in G$. Now, let $\Gamma := \{1, 2, 3, 4\}$ and $\Delta := \Omega \setminus \Gamma$. Then G_Δ is transitive on the set Γ because $g_1, g_3, g_1 g_3 \in G_\Delta$. Since by assumption $|\Omega| \geq 9$, we have $|\Gamma| = 4 < \frac{1}{2}|\Omega|$, and so it follows from a result of Marggraf (cf. [3] pg. 35) that $G \geq A_n$.

Case 1: $\#\mathrm{supp}(b_2)(a_1 b_1) = 1$. There are two cases to consider here: either i) $\#\mathrm{supp}(b_2)(a_1) = 1$ and $\#\mathrm{supp}(b_2)(b_1) = 0$ or ii) $\#\mathrm{supp}(b_2)(a_1) = 0$ and $\#\mathrm{supp}(b_2)(b_1) = 1$. In either case, we claim that G contains a 5-cycle. If we have i), then up to conjugacy, $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (13)(25)$ which gives $g_1 g_2 = (14325) \in G$. On the other hand, if we have ii), then up to conjugacy, $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (13)(45)$ which gives $g_1 g_2 = (14532) \in G$. So, if $\#\mathrm{supp}(b_1)(a_2) = 1$ and $\#\mathrm{supp}(b_2)(a_1 b_1) = 1$ then G contains a 5-cycle. By Netto (cf. [2] pg. 93), a primitive group of degree n which contains a p-cycle of order $p < \frac{2n}{3}$ contains the alternating group. In the case where $p = 5$ this is $15 < 2n$. Since by assumption $n \geq 9$, the inequality holds and so $G \geq A_n$.

Case 2: $\#\mathrm{supp}(b_2)(a_1 b_1) = 2$. We cannot have $\#\mathrm{supp}(b_2)(a_1) = 2$ because condition (1) and $b_2 = a_1$ would imply that b_2 and a_2 are not disjoint. Similarly, we cannot have $\#\mathrm{supp}(b_2)(b_1) = 2$ because $\#\mathrm{supp}(b_1)(a_2) = 1$ and $b_2 = b_1$ would also imply that b_2 and a_2 are not disjoint. Therefore, there is only one case to consider: $\#\mathrm{supp}(b_2)(a_1) = 1$ and $\#\mathrm{supp}(b_2)(b_1) = 1$. Up to conjugacy, this is $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (13)(24)$. Thus, we have $g_3 := g_1 g_2 = (14)(23) \in G$. Now, as in Case 0 above, let $\Gamma := \{1, 2, 3, 4\}$ and $\Delta := \Omega \setminus \Gamma$. Then, $g_1, g_2, g_3 \in G_\Delta$ and G_Δ is transitive on Γ. Since

$|\Gamma| = 4$, the above cited result of Marggraf gives that $G \geq A_n$.

Since the preceding cases exhaust the possibilities for $\#\text{supp}(b_2)(a_1 b_1) \in \{0, 1, 2\}$, Claim 1 is proved. We turn now to Claim 2.

Claim 2: $\#\text{supp}(b_1)(a_2) = 0 \implies G \geq A_n$ unless (2).

As before, we divide the argument into subcases according to the value of $\#\text{supp}(b_2)(a_1 b_1) \in \{0, 1, 2\}$. Since (2) is included in the case $\#\text{supp}(b_2)(a_1 b_1) = 1$, our first task is to show that if $\#\text{supp}(b_2)(a_1 b_1) \in \{0, 2\}$ then $G \geq A_n$.

Case 0: $\#\text{supp}(b_2)(a_1 b_1) = 0$. Up to conjugacy, we have $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (15)(67)$. Thus, $(g_1 g_2)^2 = (125) \in G$. By a well-known result, if a primitive group contains a 3-cycle then $G \geq A_n$ (cf. [3] pg. 34).

Case 2: $\#\text{supp}(b_2)(a_1 b_1) = 2$. We cannot have $\#\text{supp}(b_2)(a_1) = 2$ because (1) $\#\text{supp}(a_1)(a_2) = 1$ and $b_2 = a_1$ would imply that a_2 and b_2 are not disjoint. Thus, there are two subcases to consider: either i) $\#\text{supp}(b_2)(a_1) = 1$ and $\#\text{supp}(b_2)(b_1) = 1$ or ii) $\#\text{supp}(b_2)(a_1) = 0$ and $\#\text{supp}(b_2)(b_1) = 2$. If we have i) then up to conjugacy, $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (15)(23)$. Thus, $g_1 g_2 = (12)(34)(15)(23) = (15243) \in G$. While, if we have ii) then up to conjugacy, $g_1 = a_1 b_1 = (12)(34)$, $g_2 = a_2 b_2 = (15)(34)$ which gives $g_1 g_2 = (152) \in G$. So, if $\#\text{supp}(b_1)(a_2) = 0$ and $\#\text{supp}(b_2)(a_1 b_1) = 2$ then G either contains a 5-cycle or a 3-cycle. As shown previously, the presence of either implies that $G \geq A_n$.

Thus, from the preceding two cases, we conclude that if $\#\text{supp}(b_1)(a_2) = 0$ and $\#\text{supp}(b_2)(a_1 b_1) \in \{0, 2\}$ then $G \geq A_n$. The final case to consider is $\#\text{supp}(b_2)(a_1 b_1) = 1$ where we show that $G \geq A_n$ unless (2) holds.

Case 1: $\#\text{supp}(b_2)(a_1 b_1) = 1$. Here, there are two cases to consider: either i) $\#\text{supp}(b_2)(a_1) = 1$ and $\#\text{supp}(b_2)(b_1) = 0$ or ii) $\#\text{supp}(b_2)(a_1) = 0$ and $\#\text{supp}(b_2)(b_1) = 1$. If we can show that the former implies $G \geq A_n$ then we will have proven the proposition because ii) is precisely (2). If we have i) then up to conjugacy, $g_1 = a_1 b_1 = (12)(34)$ and $g_2 = a_2 b_2 = (15)(26)$. Also in the group is the element $g_3 := g_1 g_2 g_1 = (25)(16)$ and consequently the element $g_3 g_2 = (25)(16)(15)(26) = (12)(56)$. Now, let $\Gamma := \{1, 2, 5, 6\}$ and $\Delta := \Omega \setminus \Gamma$. Since, $g_2, g_3, g_3 g_2 \in G_\Delta$, G_Δ is transitive on the set Γ. As before, $|\Gamma| = 4$ and the result of Marggraf cited above gives $G \geq A_n$.

Thus, we have shown that if (1) holds then $G \geq A_n$ unless (2) holds. □

Corollary 1. *Let G be a primitive permutation group of degree $n \geq 9$ which contains a $(2, 2)$ cycle $g_1 = a_1 b_1$. Then G contains a second $(2, 2)$ cycle $g_2 = a_2 b_2$ such that* (1) *holds. Moreover, $G \geq A_n$ unless* (2) *holds.*

Proof. Let G act on the set $\Omega := \{1, .., n\}$. Without loss of generality, we can assume that $a_1 = (12)$. By a lemma of Rudio (cf. [2] pg. 78), the primitivity of G implies that there exists an $h \in G$ such that $1^h \in \{1, 2\}$ while $2^h \notin \{1, 2\}$. Let $a_2 := h a_1 h^{-1} = (1^h\, 2^h)$ and $b_2 := h b_1 h^{-1}$. Then, $g_2 := h g_1 h^{-1} = a_2 b_2 \in G$ and by our choice of h we have (1) $\#\text{supp}(a_1)(a_2) = 1$. By Proposition 1, $G \geq A_n$ unless (2) holds as well. □

Remark 1. Proposition 1 roughly corresponds to cases A and B of Netto's argument. Some specific differences in our formulation are the appeal to a result of Marggraf, and the fact that a 5-cycle in a primitive group of degree ≥ 9 implies that the group contains the alternating group. Although new, these are only simplifications over Netto; his treatement of the third case is what in fact necessitated our new formulation.

In his case C analysis on pg. 136, Netto lists a number of possible cases for a $(2, 2)$ cycle. One of which is $(x_1 x_m)(x_n x_p)$ where $m, n, p \in \{1, ..n\} \setminus \{1, 2, 5\}$. On the following page, Netto claims that in every case a proper combination of this element with the other elements already determined to be in the group, $(x_1 x_2)(x_3 x_4)$, $(x_1 x_5)(x_3 x_6)$, and $(x_2 x_5)(x_4 x_6)$, results in a 7-cycle. However, if $m = 3$, $n = 7$ and $p = 8$ then no such 7-cycle appears in any combination of these elements; in fact, the permutation group generated by these elements is of order 48 which cannot contain a 7-cycle. It is not entirely clear from the exposition whether Netto had a different range in mind for the indices or if this case was simply overlooked. In either case, a new argument was needed.

Since Netto's case C originally began with $(x_1 x_2)(x_3 x_4)$ and $(x_1 x_5)(x_3 x_6)$ being in the group and these elements satisfy conditions (1) and (2) from above, we have given a new proof that such conditions imply that $G \geq A_n$. This proof appears as:

Proposition 2. *Let G be a primitive permutation group of degree $n \geq 9$ acting on a set Ω. If G contains a subset $T_k := \{g_1, g_2, ..., g_k\}$ with $k \geq 2$, such that the following conditions hold:*

1. *$g_i = a_i b_i$ is a $(2, 2)$ cycle for $1 \leq i \leq k$,*
2. *$\exists\, t \in \Omega$ s.t. for $i \neq j, 1 \leq i, j \leq k$, $supp(a_i)(a_j) = \{t\}$,*
3. *$\Delta_a^k \cap \Delta_b^k = \emptyset$ where $\Delta_a^k := \bigcup_{i=1}^k supp(a_i)$ and $\Delta_b^k := \bigcup_{i=1}^k supp(b_i)$,*

then $G \geq A_n$.

Proof. Let G be a primitive permutation group of degree $n \geq 9$ and let T_k be a subset of G that satisfies the hypotheses of the proposition.

Suppose that $G \ngeq A_n$. We begin by establishing that the primitivity of G implies the existence of an element $g_{k+1} = a_{k+1} b_{k+1} \in G$ such that g_{k+1} is a $(2, 2)$ cycle and $\text{supp}(a_i)(a_j) = \{t\}$ for $i \neq j$, $1 \leq i, j \leq k + 1$. In other words, $T_{k+1} := T_k \cup \{g_{k+1}\}$ satisfies the first two conditions of the proposition. We then show that because we have supposed $G \ngeq A_n$, T_{k+1} must also satisfy the third condition of the proposition. To complete the proof, we show that this implies a contradiction and hence we must have $G \geq A_n$.

To begin, we have $g_k = a_k b_k = (t\, u)(v\, w)$ where $u, v, w \in \Omega$. Note that $t \in \text{supp}(a_k)$ because $g_k \in T_k$ and T_k satisfies condition 2 of the proposition. Since $\Delta_a^k \neq \Omega$ by condition 3, the lemma of Rudio implies that there exists $h \in G$ such that $t^h \in \Delta_a^k$ while $u^h \notin \Delta_a^k$. Consider $h a_k h^{-1} = (t^h\, u^h)$ and $h b_k h^{-1} = (v^h\, w^h)$. If $t^h = t$ then let $a_{k+1} := h a_k h^{-1}$ and $b_{k+1} := h b_k h^{-1}$. Then, $g_{k+1} := a_{k+1} b_{k+1} = h g_k h^{-1} = (t\, u^g)(v^g\, w^g) \in G$ is a $(2, 2)$ cycle, and $\text{supp}(a_i)(a_j) = \{t\}$ for $i \neq j$, $1 \leq i, j \leq k+1$. Thus, $T_{k+1} := T_k \cup \{g_{k+1}\}$ satisfies the first two conditions of the proposition.

We now consider the case $t^h \neq t$ and show that here too the set $T_{k+1} := T_k \cup \{g_{k+1}\}$ satisfies the first two conditions of the proposition. If $t^h \neq t$ then we still have $t^h \in$

$\mathrm{supp}(a_r)$ for some $g_r = a_r b_r \in T_k$; in fact, $a_r = (t^h\, t)$ because $t \in \mathrm{supp}(a_r)$. In this case, let a_{k+1} be the transposition that results from first conjugating a_k by h and then by g_r. Similarly, let b_{k+1} be the transposition that results from first conjugating b_k by h and then by g_r. Then, $g_{k+1} := a_{k+1}b_{k+1} \in G$ and $a_{k+1} = (t^{hg_r}\, u^{hg_r})^{\dagger}$. Now, $t^{hg_r} = t^{ha_r b_r} = t^{b_r} = t$ because if b_r did not fix t then g_r would not be a $(2,2)$ cycle contrary to assumption (i.e. a_r and b_r would not be disjoint). So, $a_{k+1} = (t\, u^{hg_r})$.

Now, consider u^{hg_r}. We want to show that $u^{hg_r} \notin \Delta_a^k$ because this implies that $\mathrm{supp}(a_i)(a_j) = \{t\}$ for $i \neq j$, $1 \leq i, j \leq k+1$. Since $u^h \notin \Delta_a^k$, we know that a_r fixes u^h so $u^{hg_r} = u^{hb_r}$. Now, either $u^h \notin \mathrm{supp}(b_r)$ or $u^h \in \mathrm{supp}(b_r)$. If $u^h \notin \mathrm{supp}(b_r)$ then b_r fixes u^h as well and $u^{hg_r} = u^h \notin \Delta_a^k$. On the other hand, if $u^h \in \mathrm{supp}(b_r)$ then b_r being a transposition, $b_r = (u^h u^{hb_r})$ and so, $u^{hg_r} = u^{hb_r} \notin \Delta_a^k$ because if $u^{hb_r} \in \Delta_a^k$ then $u^{hb_r} \in \Delta_a^k \cap \Delta_b^k$ contrary to assumption. This shows that as in the case where $t^h = t$, we have that $g_{k+1} = a_{k+1}b_{k+1} \in G$ is a $(2,2)$ cycle, and $\mathrm{supp}(a_i)(a_j) = \{t\}$ for $i \neq j$, $1 \leq i, j \leq k+1$. Hence, in either case, T_{k+1} satisfies the first two conditions of the proposition.

The next step in the proof is to show that because of our supposition that $G \ngeq A_n$, T_{k+1} must also satisfy the third condition; that is, $\Delta_a^{k+1} \cap \Delta_b^{k+1} = \emptyset$. The fact that T_{k+1} satisfies all three of the conditions will then be shown to imply a contradiction.

To show $\Delta_a^{k+1} \cap \Delta_b^{k+1} = \emptyset$, note that for distinct $g_i, g_j \in T_{k+1}$, $\#\mathrm{supp}(a_i)(a_j) = 1$ so g_i and g_j satisfy condition (1) in Proposition 1. And since we've assumed that $G \ngeq A_n$, Proposition 1 gives us (2): $\#\mathrm{supp}(b_i)(a_j) = 0$, $\#\mathrm{supp}(a_i)(b_j) = 0$, and $\#\mathrm{supp}(b_i)(b_j) = 1$. Now, since this applies to any distinct $g_i, g_j \in T_{k+1}$, we must have $\Delta_a^{k+1} \cap \Delta_b^{k+1} = \emptyset$. Thus, T_{k+1} satifies all three of the conditions in the proposition. What remains to be shown is that this leads to a contradiction.

The contradiction follows from the fact that $\#\mathrm{supp}(T_{k+1}) \geq \#\mathrm{supp}(T_k) + 1$ which we prove presently. First of all, $\#\mathrm{supp}(T_{k+1}) \geq \#\mathrm{supp}(T_k \cup \{a_{k+1}\})$ because $T_{k+1} = T_k \cup \{g_{k+1}\}$. Now, we need to show that $\#\mathrm{supp}(T_k \cup \{a_{k+1}\}) = \#\mathrm{supp}(T_k) + 1$. We do so by showing that there is precisely one element in $\mathrm{supp}(a_{k+1})$ that is not in $\mathrm{supp}(T_k)$; that is, $\#\mathrm{supp}(a_{k+1})(T_k) = 1$. This follows from the fact that T_{k+1} satisfies the three conditions of the proposition. More precisely, from $\Delta_a^{k+1} \cap \Delta_b^{k+1} = \emptyset$ we get $\mathrm{supp}(a_{k+1}) \cap \Delta_b^k = \emptyset$, and from $\mathrm{supp}(a_{k+1})(a_i) = \{t\}$ for $1 \leq i \leq k$ we get $\mathrm{supp}(a_{k+1}) \cap \Delta_a^k = \{t\}$. Since $\Delta_a^k \cup \Delta_b^k = \mathrm{supp}(T_k)$, these imply that $\mathrm{supp}(a_{k+1})(T_k) = \{t\}$. Hence,

$$\#\mathrm{supp}(T_{k+1}) \geq \#\mathrm{supp}(T_k \cup \{a_{k+1}\}) = \#\mathrm{supp}(T_k) + 1. \tag{3}$$

With this inequality in hand, the contradiction is derived as follows. By assuming that $G \ngeq A_n$, $T_k \subseteq G$ implies $T_{k+1} \subseteq G$ where T_{k+1} also satisfies the hypotheses of the proposition. Thus, by iteration, what we in fact have is that $T_k \subseteq G$ implies $T_{k+s} \subseteq G$ for any $s \geq 0$ by a chain of implications. In particular, $T_k \subseteq G$ implies $T_{k+n} \subseteq G$. Then, by (3), we have $\#\mathrm{supp}(T_{k+n}) \geq \#\mathrm{supp}(T_k) + n > n$. So, $\#\mathrm{supp}(T_{k+n}) > n$. But, $T_{k+n} \subseteq G$ so we cannot have that the support of T_{k+n} is greater than the degree n of G. This is a contradiction. Hence, $G \geq A_n$. $\square$

† In symbols, this is: $a_{k+1} := g_r h a_k h^{-1} {g_r}^{-1} = (t^{hg_r}\, u^{hg_r})$ and $b_{k+1} := g_r h b_k h^{-1} {g_r}^{-1} = (v^{hg_r}\, w^{hg_r})$. Then, $g_{k+1} = g_r h g_k h^{-1} {g_r}^{-1}$. Therefore, $g_{k+1} \in G$.

Proposition 1 (more precisely, Corollary 1) and Proposition 2 immediately furnish Theorem 2:

Proof of Theorem 2. If G contains a 4-cycle then the square of that element will be a $(2,2)$-cycle so we can suppose, without loss of generality, that G contains a $(2,2)$-cycle, g_1.

By Corollary 1, we have another element g_2 in G such that if $G \not\geq A_n$ then conditions (1) and (2) hold. But if (1) and (2) hold then $T_2 := \{g_1, g_2\}$ satisfies the hypotheses of Proposition 2, and so $G \geq A_n$. □

With this result in hand, we now turn to the specific case of $n = 7$. Here, we prove a more general result than is needed to establish Theorem 1; namely,

Proposition 3. *If $G \leq S_7$ is transitive and contains a 4-cycle, then $G = S_7$.*

In doing so, we make use of the following well-known lemma:

Lemma 1. *A group of order 84 is solvable.*

Proof. Let K be a group of order $84 = 7 \cdot 4 \cdot 3$. By the Sylow Theorems, the number, n_7, of Sylow 7-subgroups of K must satisfy: $n_7 \equiv 1 \bmod 7$ and $n_7 \mid 12$. Thus, $n_7 = 1$, so the unique Sylow 7-subgroup of K is normal and by forming the quotient group $\frac{K}{P_7}$, we get $|\frac{K}{P_7}| = \frac{|K|}{|P_7|} = 12$. Hence, P_7 and $\frac{K}{P_7}$ are both solvable implying K is solvable. □

Also, we remark that, by an easy argument, a transitive group of prime degree is automatically primitive (cf. [3] pg. 16).

Proof of Proposition 3. We begin by supposing that $G \neq S_7$. Since G contains a 4-cycle and thus $G \neq A_7$, this is equivalent to supposing $G \not\geq A_7$. Now, since G is a permutation group of prime degree, we have from Galois (cf. [3] pg. 29) that G is solvable iff for two distinct points of $\{1, .., 7\}$ the only element which fixes both is the identity. The 4-cycle in G, however, fixes three distinct points and so G is insolvable. By Burnside (cf. [3] pg. 29), every insolvable transitive group of prime degree is 2-transitive. Hence, G is 2-transitive.

By a result of Bochert (cf. [3] pg. 41), a primitive group $G \not\geq A_n$ satisfies:

$$|S_n : G| \geq [\tfrac{n+1}{2}]!$$

With $n = 7$ this implies $|S_7 : G| \geq 4!$ and hence, $|G| \leq 210$. As a lower bound, we have $60 \leq |G|$ because G is insolvable. By Wielandt (cf. [3] pg. 20) the order of a k-fold transitive group of degree n is divisible by $n(n-1)...(n-k+1)$. In our case, G is at least 2-transitive, so $7(7-1) = 42$ divides $|G|$. Together, these conditions give $|G| \in \{84, 126, 168, 210\}$.

Now, by Lemma 1, $|G| \neq 84$ because G is insolvable. Furthermore, the presence of the 4-cycle means $|G|$ must be divisible by 4 so $|G| \neq 126, 210 \implies |G| = 168$. If $|G| = 168$ then we claim G must be simple. Suppose G had a proper normal subgroup H. If $3 \leq |H| \leq 56$ then by a straight cardinality argument both H and $\frac{G}{H}$ must be solvable. On the other hand, if $|H| \in \{2, 84\}$ then by Lemma 1, both H and $\frac{G}{H}$ are again solvable. Since G is insolvable, these would imply a contradiction and so G must be simple.

We now show that if G is simple then $G \leq A_7$. Let G' and S_7' be the commutator subgroups for G and S_7 respectively. Then, $G' \leq S_7'$ because $G \leq S_7$. Since G is nonabelian simple, $G = G'$. Furthermore, given that $S_7' = A_7$, this implies $G \leq A_7$. But G contains a 4-cycle, which is odd, so $G \nleq A_7$. This being a contradiction, our original assumption that $G \neq S_7$ must have been wrong. Hence, $G = S_7$. □

With Theorem 2 for $n \geq 9$ and the preceding Proposition 3 for $n = 7$, we are now in a position to prove our desired result, Theorem 1:

Proof of Theorem 1. If $n = 7$ then $s_4 \in G$ is a 4-cycle and by Proposition 3, $G = S_7$. If $n \geq 9$ then because s_4 has cycle decomposition $(2)^{m-3}(4)$, ${s_4}^2 \in G$ is a $(2, 2)$ cycle and $G \geq A_n$ by Theorem 2.

Moreover, if $n \equiv 1 \pmod 4$ then $m \equiv 0 \pmod 2$ and s_1, s_2, s_3 and s_4 are all even. Since G is generated by even elements, $G \leq A_n$. Together with $G \geq A_n$, this implies $G = A_n$ if $n \equiv 1 \pmod 4$.

On the other hand, if $n \equiv 3 \pmod 4$, then $m \equiv 1 \pmod 2$ and s_1, s_2, s_3 and s_4 are all odd. Since G contains odd elements, $G \neq A_n$. Together with $G \geq A_n$ this implies $G = S_n$ if $n \equiv 3 \pmod 4$. □

References

[1] Frey, G. and Kani, E. Curves of genus 2 with elliptic differentials and associated Hurwitz spaces, preprint, 2008. To appear in: *Contemp. Math.*

[2] Netto, E. *Theory of Substitutions.* Chelsea Publishing Co., New York, 1964.

[3] Wielandt, H. *Finite Permutation Groups.* Academic Press, New York, 1964.