EXCEPTIONAL SUBGROUPS OF $\mathrm{SL}(2,F)$

DARRYL MCCULLOUGH

ABSTRACT. For $A, B \in \mathrm{SL}(2,\mathbb{C})$, R. C. Churchill gave simple conditions in terms of $\mathrm{tr}(A)$, $\mathrm{tr}(B)$, and $\mathrm{tr}(AB)$ to determine whether the image of the subgroup $\langle A, B\rangle$ in $\mathrm{PSL}(2,\mathbb{C})$ is isomorphic to A_4, S_4, or A_5. We prove that the same conditions work for $\mathrm{SL}(2,F)$ for any field F, except when the image is A_5 and F has characteristic 3, 11, 19, or 29.

INTRODUCTION

Some work of R. C. Churchill [1] includes a characterization of two-generator subgroups of $\mathrm{SL}(2,\mathbb{C})$ that generate a subgroup of $\mathrm{PSL}(2,\mathbb{C})$ isomorphic to either A_4, S_4, or A_5. It may be useful to have an extension of this characterization to $\mathrm{SL}(2,F)$ for other F. To this end, drawing considerably on Churchill's ideas, we will prove that it extends to all fields, except for certain cases in characteristics $p = 3$, 11, 19, and 29.

To set up the statement of the main result, fix a field F of characteristic p, possibly 0. Replace F by its algebraic closure, if necessary, to assume that it is algebraically closed. Write $\sqrt{2}$ for one of the nonzero solutions of $x^2 = 2$, which exist only when $p \neq 2$. Write μ_1 for one of the solutions of $x^2-x-1 = 0$, and put $\mu_2 = \mu_1^{-1} = \mu_1-1$. Note that $-\mu_2$ is the other solution of $x^2 - x - 1 = 0$, and that μ_2 and $-\mu_1$ are the solutions of $x^2 + x - 1 = 0$. Define $T_2 = \{0\}$, $T_3 = \{\pm 1\}$, $T_4 = \{\pm\sqrt{2}\}$, and $T_5 = \{\pm\mu_1, \pm\mu_2\}$. It is an elementary fact (see section 1) that for $2 \leq n \leq 5$ and $A \in \mathrm{SL}(2,F)$ ($A \neq \pm I$), A has order n in $\mathrm{PSL}(2,F)$ if and only $\mathrm{tr}(A) \in T_n$. In particular, if at least two of $\mathrm{tr}(A)$, $\mathrm{tr}(B)$, and $\mathrm{tr}(AB)$ are 0, then the subgroup that A and B generate in $\mathrm{PSL}(2,F)$ is dihedral or is a subgroup of $C_2 \times C_2$.

Our Main Theorem involves the trace of the commutator $[A, B]$ of two elements of $\mathrm{SL}(2,F)$. It can be expressed in terms of $\mathrm{tr}(A)$, $\mathrm{tr}(B)$, and $\mathrm{tr}(AB)$ using the well-known Fricke trace identity

$$\mathrm{tr}([A,B]) = \mathrm{tr}^2(A) + \mathrm{tr}^2(B) + \mathrm{tr}^2(AB) - \mathrm{tr}(A)\,\mathrm{tr}(B)\,\mathrm{tr}(AB) - 2\ .$$

Finally, write $\langle A, B\rangle$ for the subgroup of $\mathrm{SL}(2,F)$ generated by A and B, and $P\colon\ \mathrm{SL}(2,F) \to \mathrm{PSL}(2,F)$ for the canonical projection. In the statement of the Main Theorem and throughout our work, two groups are considered to be equal whenever they are isomorphic.

Date: June 14, 2005.

2000 *Mathematics Subject Classification.* Primary 20G15; Secondary 20F29.

Key words and phrases. SL, projective, tetrahedral, octahedral, icosahedral, alternating, finite, trace, commutator.

Main Theorem. *Let* $A, B \in \mathrm{SL}(2, F)$*, with no more than one of* $\mathrm{tr}(A)$*,* $\mathrm{tr}(B)$*, or* $\mathrm{tr}(AB)$ *equal to* 0*. Then*

1) $P(\langle A, B\rangle) = A_4$ *if and only if* $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB) \in T_2 \cup T_3$ *and* $\mathrm{tr}([A, B]) = 0$*.*
2) $P(\langle A, B\rangle) = S_4$ *if and only if* $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB) \in T_2 \cup T_3 \cup T_4$ *and* $\mathrm{tr}([A, B]) = 1$*.*
3) *Apart from the exceptional cases listed below,* $P(\langle A, B\rangle) = A_5$ *if and only if* $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB) \in T_2 \cup T_3 \cup T_5$ *and* $\mathrm{tr}([A, B]) \in \{-\mu_2, 1, \mu_1\}$*. In each of the following exceptional cases, one can find examples of pairs* A, B *with* $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB) \in T_2 \cup T_3 \cup T_5$*, where* $P(\langle A, B\rangle)$ *does equal* A_5*, and where it does not equal* A_5*:*
   (a) $p \in \{3, 11, 29\}$ *and* $\mathrm{tr}([A, B]) \in \{\mu_1, -\mu_2\}$*.*
   (b) $p = 19$ *and* $\mathrm{tr}([A, B]) = 1$*.*

In the exceptional cases, it is easy to tell by examination of $\mathrm{tr}(A)$, $\mathrm{tr}(B)$, and $\mathrm{tr}(AB)$ whether or not $P(\langle A, B\rangle) = A_5$. The method requires information from the proof of the Main Theorem, so we will defer its explanation until the very end of this paper.

Our proof of the Main Theorem uses only elementary trace identities and calculations, with occasional assistance from the GAP package of computer algorithms [2]. Unfortunately, a large number of cases must be considered; we hope that our presentation has organized them in a way that minimizes the pain.

Throughout, we freely use the elementary trace identity $\mathrm{tr}(AB^{-1}) + \mathrm{tr}(AB) = \mathrm{tr}(A)\,\mathrm{tr}(B)$ and its consequences (such as $\mathrm{tr}(A^2) = \mathrm{tr}(A)^2 - 2$ and the Fricke trace identity).

1. Preliminaries

The following facts about elements $A \in \mathrm{SL}(2, F)$ ($A \neq \pm I$) are easily checked:

1) $A^2 = I$ if and only if $p = 2$ and $\mathrm{tr}(A) = 0$.
2) $A^2 = -I$ if and only if $\mathrm{tr}(A) = 0$.
3) $A^3 = \pm I$ if and only if $\mathrm{tr}(A) = \mp 1$.
4) $A^4 = -I$ if and only if $\mathrm{tr}(A)^2 = 2$.
5) $A^5 = \pm I$ if and only if $\mathrm{tr}(A) = \mp \mu_1$ or $\mathrm{tr}(A) = \pm \mu_2$.

These show that $P(A)$ has order n if and only if $\mathrm{tr}(A) \in T_n$.

We will use the following, which is part of Proposition 8.1 of [1].

Proposition 1.1. *In the following,* g *and* h *denote elements of a certain group, for which* $g \notin \langle h\rangle$ *and* $h \notin \langle g\rangle$*. Then*

1) *If* $g, h \in A_4$*, then* $\langle g, h\rangle = A_4$ *if and only if at least one of* g *and* h *has order* 3*.*
2) *If* $g, h \in S_4$*, then* $\langle g, h\rangle = S_4$ *if and only if at least one of* g*,* h*, and* gh *has order* 4*, and at most one has order* 2*.*
3) *If* $g, h \in A_5$*, then* $\langle g, h\rangle = A_5$ *if and only if at least one of* g*,* h*, and* gh *has order* 5*, and at most one has order* 2*.*

It will be convenient to use Nielsen equivalence. The *Nielsen group for pairs* is

$$\mathbb{U} = C_2 * C_2 * C_2 = \langle t, u, v \mid t^2, u^2, v^2 \rangle \ .$$

If K is any group, $\mathbb{U}$ acts on the set of pairs $K \times K$ as follows.

1. $t(A, B) = (A^{-1}, B)$
2. $u(A, B) = (B, A)$
3. $v(A, B) = (A^{-1}, AB)$

The orbits of the action of $\mathbb{U}$ on $K \times K$ are called *Nielsen equivalence classes* of pairs. Put more concretely, pairs are Nielsen equivalent when one can be obtained from the other by any sequence of operations of replacing an element by its inverse, interchanging the two elements of the pair, or pre- or post-multiplying one element by the other, or by the inverse of the other. Note that Nielsen equivalent pairs generate the same subgroup of K.

An F-triple is an element of $F \times F \times F$. The Nielsen group acts on the set of F-triples as follows:

1) $t(\alpha, \beta, \gamma) = (\alpha, \beta, \alpha\beta - \gamma)$
2) $u(\alpha, \beta, \gamma) = (\beta, \alpha, \gamma)$
3) $v(\alpha, \beta, \gamma) = (\alpha, \gamma, \beta)$

This action is induced from the action of $\mathbb{U}$ on $\mathrm{SL}(2, F) \times \mathrm{SL}(2, F)$ via the function Tr defined by $\mathrm{Tr}(A, B) = (\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB))$; that is, if $\mathrm{Tr}(A, B) = (\alpha, \beta, \gamma)$, then $t \circ \mathrm{Tr} = \mathrm{Tr} \circ t$, $u \circ \mathrm{Tr} = \mathrm{Tr} \circ u$, and $v \circ \mathrm{Tr} = \mathrm{Tr} \circ v$. For u and v this is obvious, and for t it is simply the identity that $\mathrm{tr}(A^{-1}B) = \mathrm{tr}(A)\,\mathrm{tr}(B) - \mathrm{tr}(AB)$. We declare two F-triples to be equivalent if they lie in the same $\mathbb{U}$-orbit. In particular, permuting the entries of a triple produces an equivalent triple.

From now on, we assume that $K = \mathrm{SL}(2, F)$. For this case, we further declare (A, B) to be equivalent to each of $(-A, B)$, $(A, -B)$, and $(-A, -B)$. Via Tr, these induce the further equivalences of (α, β, γ) with each of $(-\alpha, \beta, -\gamma)$, $(\alpha, -\beta, -\gamma)$, and $(-\alpha, -\beta, \gamma)$. Both equivalence relations are denoted by the symbol $\sim$.

For notational convenience, we define the Fricke polynomial $Q\colon F^3 \to F$ by

$$Q(\alpha, \beta, \gamma) = \alpha^2 + \beta^2 + \gamma^2 - \alpha\,\beta\,\gamma - 2 \ ,$$

so that $\mathrm{tr}([A, B]) = Q(\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB))$.

It is straightforward to check that if $A, B \in \mathrm{SL}(2, F)$ and $(A, B) \sim (A', B')$, then $P(\langle A, B \rangle) = P(\langle A', B' \rangle)$. Moreover, $\mathrm{tr}([A, B]) = \mathrm{tr}([A', B'])$, and consequently

$$Q(\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)) = Q(\mathrm{tr}(A'), \mathrm{tr}(B'), \mathrm{tr}(A'B')) \ .$$

Thus in the proof of the Main Theorem, we may replace (A, B) by any equivalent pair, or $(\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB))$ by any equivalent triple, while assuming that $P(\langle A, B \rangle)$ and $\mathrm{tr}([A, B])$ are unchanged.

2. Proof of the "only if" direction of the Main Theorem

In the course of the proof, we will develop some additional information about generating pairs of exceptional groups. Since some of it could be of independent interest, we will organize most of the argument as a pair of lemmas and a corollary. The lemmas are certainly well-known; in particular Nielsen equivalence for generating pairs of A_5 was first analyzed in [4].

Lemma 2.1. *Let H be A_4 or S_4. Then any two generating pairs of H are Nielsen equivalent. Consequently:*

1) *Any generating pair of A_4 is Nielsen equivalent to a pair (g, h) for which $g^3 = h^3 = (gh)^2 = 1$.*
2) *Any generating pair of S_4 is Nielsen equivalent to a pair (g, h) for which $g^4 = h^3 = (gh)^2 = 1$.*

Proof. For A_4, we may assume using proposition 1.1(a) that g has order 3, and by conjugation (which can be achieved by Nielsen equivalence) and possibly replacing g by g^{-1}, we may assume that $g = (123)$. If h has order 2, replace it by gh which has order 3. Conjugating h by powers of g and possibly replacing h by h^{-1}, we may assume that $h = (431)$. That is, every generating pair is Nielsen equivalent to $((123), (431))$, which obey the relations in (a).

For S_4, we may similarly assume using proposition 1.1(b) that $g = (1234)$. Not both h and gh can have order 4, since $S_4/A_4 \cong C_2$, so we may assume that h has order 3. Conjugating h by powers of g and possibly replacing h by h^{-1}, we may assume that $h = (321)$. That is, every generating pair is Nielsen equivalent to $((1234), (321))$, which obey the relations in (b). $\square$

Lemma 2.2. *Let H be A_5. Then any generating pair of H is Nielsen equivalent to exactly one of the pairs* $((12345), (124))$*,* $((12345), (12354))$*, or* $((12354), (125))$.

Proof. By proposition 1.1, we may assume that g is a 5-cycle. By conjugation we may make it one of (12345) or (12354); assume for now that it is the first. Using lemma 8.2 of [1], we may assume that h is not a 5-cycle.

Suppose first that h has order 2. Conjugating h by g, we may assume that h is either (12)(34), (13)(24), or (14)(23). The latter case is impossible since then, gh has order 2 and $\langle g, h\rangle$ is dihedral. In the first two cases, gh and respectively g^2h are 3-cycles. Replacing the pair by (g, gh) or by (g, g^2h), we may assume that h is a 3-cycle. Conjugating h by g, and possibly replacing h by h^{-1}, we may assume that h is either (123) or (124). If $h = (124)$, we have the first pair, while if $h = (123)$, then (g, g^3hg^3) is the second pair.

For the case when g is conjugate to (12354), a very similar argument (e. g. just conjugate everything in the previous argument by (45)) shows that (g, h) is Nielsen equivalent to the second or third pair.

To see that these three pairs are not Nielsen equivalent, regard A_5 as $\mathrm{SL}(2, 4)$. We have $\{\mu_1, \mu_2\} = \mathbb{F}_4 - \{0, 1\}$, and we choose notation so that the matrix corresponding to (12345) has trace μ_1 and the one corresponding to (12354) has trace μ_2. Then,

1) If $(A, B) \in \mathrm{SL}(2,4) \times \mathrm{SL}(2,4)$ corresponds to $((12345),(124))$, then $\mathrm{tr}([A,B]) = Q(\mu_1, 1, 0) = \mu_1^2 + 1 = \mu_1$.
2) If $(A, B) \in \mathrm{SL}(2,4) \times \mathrm{SL}(2,4)$ corresponds to $((12345),(12354))$, then $\mathrm{tr}([A,B]) = Q(\mu_1, \mu_2, 0) = \mu_1^2 + \mu_2^2 = 1$.
3) If $(A, B) \in \mathrm{SL}(2,4) \times \mathrm{SL}(2,4)$ corresponds to $((12354),(125))$, then $\mathrm{tr}([A,B]) = Q(\mu_2, 1, 0) = \mu_2^2 + 1 = \mu_2$.

Since $\mathrm{tr}([A,B]))$ is an invariant of the Nielsen equivalence class, no two of the three pairs are Nielsen equivalent. □

Corollary 2.3. *Let $A, B \in \mathrm{SL}(2,F)$, and suppose that $P(\langle A, B\rangle) = A_5$. Then $Q(\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)) \in \{\mu_1, 1, -\mu_2\}$. Moreover,*

(a) *(A, B) is Nielsen equivalent to a pair for which $P(A)^5 = P(B)^3 = P(AB)^2 = P(I)$ if and only if $\mathrm{tr}([A,B]) \in \{\mu_1, -\mu_2\}$.*
(b) *(A, B) is Nielsen equivalent to a pair for which $P(A)^5 = P(B)^5 = P(AB)^2 = P(I)$ and $P(A)$ is not conjugate to $P(B)$ if and only if $\mathrm{tr}([A,B]) = 1$.*

Proof. If we can change (A, B) by equivalence so that $P(A)^5 = P(B)^3 = P(AB)^2 = P(I)$, then the associated traces are $(\pm\mu_1, \pm 1, 0)$ or $(\pm\mu_2, \pm 1, 0)$, and we find that $\mathrm{tr}([A,B]) = \mu_1$ and $\mathrm{tr}([A,B]) = -\mu_2$ respectively. If not, then by lemma 2.2 we may assume that $P(A)^5 = P(B)^5 = P(AB)^2 = P(I)$ with $P(A)$ and $P(B)$ not conjugate in A_5. Since F is algebraically closed, elements of $\mathrm{SL}(2,F)$ having the same trace are conjugate provided that the trace is not ± 2. If $p \neq 5$, then μ_1 and μ_2 are not ± 2, and it follows that one of $\mathrm{tr}(A)$ or $\mathrm{tr}(B)$ is $\pm\mu_1$ and the other is $\pm\mu_2$. Therefore $\mathrm{tr}([A,B]) = \mu_1^2 + \mu_2^2 - 2 = \mu_1 - \mu_2 = 1$. If $p = 5$, then $\pm\mu_1 = \pm\mu_2 = \pm 2$, and $\mathrm{tr}([A,B]) = 4 + 4 - 2 = 1$ for all possibilities. □

We remark that $\mu_1 = -\mu_2$ if and only if $p = 5$ (in which case both equal 3), so $\mathrm{tr}([A,B])$ fails to distinguish the two Nielsen classes in part (a) if and only if $p = 5$.

Now we can deduce the only if direction of the Main Theorem. If $P(\langle A, B\rangle)$ is one of A_4, S_4, or A_5, then by consideration of the orders of elements in these three groups, it is immediate that the traces of A and B lie in the specified sets.

If $P(\langle A, B\rangle) = A_4$, then $P([A,B])$ lies in the commutator subgroup of A_4, which consists of involutions, so $\mathrm{tr}([A,B]) = 0$.

If $P(\langle A, B\rangle) = S_4$, then by lemma 2.1 we may change (A, B) by Nielsen equivalence to assume that $P(A)^4 = P(B)^3 = P(AB)^2 = P(I)$, in which case $\mathrm{tr}([A,B]) = Q(\pm\sqrt{2}, \pm 1, 0) = 1$.

If $P(\langle A, B\rangle) = A_5$, then corollary 2.3 completes the proof.

3. Proof of the "if" direction of the Main Theorem

In this section, we write α, β, and γ for $\mathrm{tr}(A)$, $\mathrm{tr}(B)$, and $\mathrm{tr}(AB)$ respectively.

Assume first that the conditions in part 1) hold. Since no two of α, β, and γ can be 0, we may use equivalence of triples to assume that $\alpha = \beta = 1$. The condition that $Q(1, 1, \gamma) = \mathrm{tr}([A, B]) = 0$ then forces $\gamma = 0$ or $\gamma = 1$. If $\gamma = 0$, then $P(A)^3 = P(B)^3 = P(AB)^2 = I$ so $P(\langle A, B\rangle) = A_4$. If $\gamma = 1$, then $(1, 1, 1) \sim (1, 1, 0)$ and again $P(\langle A, B\rangle) = A_4$.

Assume now that the conditions in part 2) hold. We may assume using proposition 1.1 that $\alpha = \sqrt{2}$. Since no two of α, β, and γ are 0, we may assume that β is $\sqrt{2}$ or 1.

Suppose first that $\beta = \sqrt{2}$, so (α, β, γ) is of the form $(\sqrt{2}, \sqrt{2}, \gamma)$. The five possible values $(-\sqrt{2}, -1, 0, 1, \sqrt{2})$ of γ lead to the corresponding values $(4+2\sqrt{2}, 5, 2, 1, 4-2\sqrt{2})$ for $Q(\sqrt{2}, \sqrt{2}, \gamma)$. Putting these equal to 1 leads to immediate contradictions (in particular, $Q = 5$ implies that $p = 2$ and hence that $\alpha = \beta = 0$) except in the case when $\gamma = 1$. So $(\alpha, \beta, \gamma) = (\sqrt{2}, \sqrt{2}, 1) \sim (\sqrt{2}, 1, \sqrt{2}) \sim (\sqrt{2}, 1, 0)$ which gives $P(A)^4 = P(B)^3 = P(AB)^2 = P(I)$, so $P(\langle A, B\rangle) = S_4$.

Suppose now that $\beta = 1$, so (α, β, γ) is of the form $(\sqrt{2}, 1, \gamma)$, where we may assume that $\gamma \neq \sqrt{2}$. We find that $1 = Q(\sqrt{2}, 1, \gamma) = \gamma^2 - \sqrt{2}\gamma + 1$, so $\gamma = 0$ and again we conclude that $P(\langle A, B\rangle) = S_4$.

Finally, assume that the conditions in part 3) hold. By proposition 1.1 we may assume that $\alpha \in \{\mu_1, \mu_2\}$. If $\alpha = \pm\mu_2$, then we change our notation so that μ_1 becomes the other root $-\mu_2$ of $x^2 - x - 1$. So α becomes $\mp\mu_1$, and after possibly applying an equivalence to (α, β, γ), we may assume that $\alpha = \mu_1$. We will analyze the values of $Q(\mu_1, \beta, \gamma)$ for all possible cases.

Case I. $(\alpha, \beta, \gamma) = (\mu_1, \mu_1, \gamma)$

The subcases where $Q(\mu_1, \mu_1, \gamma)$ has each of the allowable values of $\mu_1, 1, -\mu_2$ are indicated by the letters A, B, and C respectively. There are further subcases corresponding to the seven possible values $(-\mu_1, -\mu_2, -1, 0, 1, \mu_2, \mu_1)$ for γ, and in our notation for cases we indicate them by the corresponding numerals 1 through 7. Thus, for example, the case when $(\alpha, \beta, \gamma) = (\mu_1, \mu_1, -\mu_2)$ and $Q(\mu_1, \mu_1, -\mu_2) = \mu_1$ is case IA2.

We calculate that $Q(\mu_1, \mu_1, \gamma) = \gamma^2 - \mu_1\gamma - \gamma + 2\mu_1$. The corresponding values of $Q(\mu_1, \mu_1, \gamma)$ are $(5\mu_1 + 2, 2\mu_1 + 2, 3\mu_1 + 2, 2\mu_1, \mu_1, 2, \mu_1)$. Thus in case IA2, we additionally know that $(\mu_1, \mu_1, \gamma) = 2\mu_1 + 2$, so we obtain the equality $2\mu_1 + 2 = \mu_1$. In our analysis of the various cases, we use the equality so obtained either to reach a contradiction showing that the subcase can never occur (as in Case IA4), or we show that the equality is an identity and hence always holds (as in Case IA5), or we show that it can only hold under certain conditions on p and μ_1 (as in Case IB1). In analyzing the cases, one frequently uses the observation that if $m\mu_1 = n$, then $n^2 = m^2\mu_1^2 = m^2\mu_1 + m^2 = mn + m^2$.

Case IA1. $Q(\mu_1, \mu_1, -\mu_1) = \mu_1$. From $5\mu_1 + 2 = \mu_1$ and the observation, we find that $p = 2$. This case is contained in case IA7 below.
Case IA2. $Q(\mu_1, \mu_1, -\mu_2) = \mu_1$. From $2\mu_1 + 2 = \mu_1$ and the observation, we find that this holds if and only if $p = 5$. But then, $-\mu_2 = \mu_1$, so this case is contained in case IA7.
Case IA3. $Q(\mu_1, \mu_1, -1) = \mu_1$. We find that $p = 2$. This case is contained in case IA5 below.
Case IA4. $Q(\mu_1, \mu_1, 0) = \mu_1$. This gives the contradiction $\mu_1 = 0$.
Case IA5. $Q(\mu_1, \mu_1, 1) = \mu_1$. This holds for all p.
Case IA6. $Q(\mu_1, \mu_1, \mu_2) = \mu_1$. This gives the contradiction that $0 = 1$.
Case IA7. $Q(\mu_1, \mu_1, \mu_1) = \mu_1$. This holds for all p.
Case IB1. $Q(\mu_1, \mu_1, -\mu_1) = 1$. This holds if and only if $(p, \mu_1) = (19, -4)$. For from $5\mu_1 + 2 = 1$ the observation gives $-5 + 25 = 1$ so p must be 19, and solving the linear equation gives $\mu_1 = -4$. And when $p = 19$, $Q(-4, -4, 4)$ is indeed 1.
Case IB2. $Q(\mu_1, \mu_1, -\mu_2) = 1$. This gives the contradiction $0 = 1$.
Case IB3. $Q(\mu_1, \mu_1, -1) = 1$. This holds if and only if $p = 5$. But then, $(\mu_1, \mu_1, -1) = (\mu_1, -\mu_2, -1) \sim (\mu_1, \mu_2, 1)$, so this is contained in case IIB5.
Case IB4. $Q(\mu_1, \mu_1, 0) = 1$. This holds if and only if $p = 5$. But then, $(\mu_1, \mu_1, 0) = (\mu_1, -\mu_2, 0) \sim (\mu_1, \mu_2, 0)$, so this is contained in case IIB4.
Case IB5. $Q(\mu_1, \mu_1, 1) = 1$. This gives the contradiction that $\mu_1 = 1$.
Case IB6. $Q(\mu_1, \mu_1, \mu_2) = 1$. This gives the contradiction that $1 = 0$.
Case IB7. $Q(\mu_1, \mu_1, \mu_1) = 1$. This gives the contradiction that $\mu_1 = 1$.
Case IC1. $Q(\mu_1, \mu_1, -\mu_1) = -\mu_2$. This holds if and only if $(p, \mu_1) = (29, -5)$.
Case IC2. $Q(\mu_1, \mu_1, -\mu_2) = -\mu_2$. This holds if and only if $p = 5$. But then, $(\mu_1, \mu_1, -\mu_2) = (\mu_1, \mu_1, \mu_1)$, so this is contained in case IA7.
Case IC3. $Q(\mu_1, \mu_1, -1) = -\mu_2$. This holds if and only if $(p, \mu_1) = (11, -3)$.
Case IC4. $Q(\mu_1, \mu_1, 0) = -\mu_2$. This holds if and only if $(p, \mu_1) = (11, 4)$.
Case IC5. $Q(\mu_1, \mu_1, 1) = -\mu_2$. This holds if and only if $p = 5$, but then it is contained in case IA7.
Case IC6. $Q(\mu_1, \mu_1, \mu_2) = -\mu_2$. Adding μ_1 to both sides of $2 = -\mu_2$ gives $2 + \mu_1 = 1$ so $\mu_1 = -1$, a contradiction.
Case IC7. $Q(\mu_1, \mu_1, \mu_1) = -\mu_2$. This holds if and only if $p = 5$, but then it is contained in case IA7.

Case II. $(\alpha, \beta, \gamma) = (\mu_1, \mu_2, \gamma)$

Since $\gamma = \pm\mu_1$ would give a triple equivalent to one of those in case I, we need only examine the subcases for which γ is one of $(*, -\mu_2, -1, 0, 1, \mu_2, *)$, where the $*$ means an ignored case. The corresponding values of $Q(\mu_1, \mu_2, \gamma)$ are $(*, 2, 3, 1, 1, 2 - 2\mu_2, *)$. We trust that the reader's appetite to examine elementary cases is by now sated, so from now on we only give summary information.

Cases IIA2, IIA4, IIA5, IIB2, IIB6, IIC2, IIC4, and IIC5. These lead to contradictions.
Case IIB3. $Q(\mu_1, \mu_2, -1) = 1$. This holds if and only if $p = 2$, which is contained in case IIB5.

Cases IIA3, IIA6, IIC3, and IIC6. These hold if and only if $p = 5$. But then these cases are contained in cases IA5, IA7, IA5, and IA7 respectively.
Case IIB4. $Q(\mu_1, \mu_2, 0) = 1$. This holds for all p.
Case IIB5. $Q(\mu_1, \mu_2, 1) = 1$. This holds for all p.
Case III. $(\alpha, \beta, \gamma) = (\mu_1, 1, \gamma)$

Since $\gamma = \pm\mu_1, \pm\mu_2$ would fall under Case I or Case II, we need only examine γ one of $(*, *, -1, 0, 1, *, *)$, with corresponding values of $Q(\mu_1, 1, \gamma)$ equal to $(*, *, 2\mu_1 + 1, \mu_1, 1, *, *)$.

Cases IIIA3, IIIA5, IIIB4, IIIC5. These lead to contradictions.
Case IIIB3. $Q(\mu_1, 1, -1) = 1$. This holds if and only if $p = 2$, which is contained in case IIIB5.
Case IIIC4. $Q(\mu_1, 1, 0) = -\mu_2$. This holds if and only if $p = 5$. But then it is contained in case IIIA4.
Case IIIC3. $Q(\mu_1, 1, -1) = -\mu_2$. This holds if and only if $p = 3$.
Case IIIA4. $Q(\mu_1, 1, 0) = \mu_1$. This holds for all p.
Case IIIB5. $Q(\mu_1, 1, 1) = 1$. This holds for all p.

We first analyze the six cases that hold for all p (the ten cases found in [1] for $\mathrm{SL}(2, \mathbb{C})$ can quickly be reduced to these six by replacement of μ_2 by $-\mu_1$ and/or applying equivalences). For each of the six cases, we will apply equivalences until the traces indicate a generating pair $P(\langle A, B\rangle)$ for which $P(A)^5 = P(B)^3 = P(AB)^2 = P(I)$.

Case IA5. $(\mu_1, \mu_1, 1) \sim (\mu_1, 1, \mu_1) \sim (\mu_1, 1, 0)$.
Case IA7. $(\mu_1, \mu_1, \mu_1) \sim (\mu_1, \mu_1, 1)$, which is case IA5.
Case IIB4. $(\mu_1, \mu_2, 0)$. Using basic trace identities, we calculate $\mathrm{tr}(B^2) = \mathrm{tr}^2(B) - 2 = \mu^2 - 2 = -\mu_1$, and $\mathrm{tr}(AB^2) = \mathrm{tr}(AB)\,\mathrm{tr}(B) - \mathrm{tr}(A) = -\mu_1$. Since $P(B)$ has order 5, we have $P(\langle A, B\rangle) = P(\langle A, -B^2\rangle)$, and from our calculations, $\mathrm{Tr}(A, -B^2) = (\mu_1, \mu_1, \mu_1)$, so case IA7 applies.
Case IIB5. $(\mu_1, \mu_2, 1) \sim (\mu_1, \mu_2, 0)$, which is case IIB4.
Case IIIA4. $(\mu_1, 1, 0)$ is immediate.
Case IIIB5. $(\mu_1, 1, 1) \sim (\mu_1, 1, \mu_1 - 1) = (\mu_1, 1, \mu_2) \sim (\mu_1, \mu_2, 1)$, which is case IIB5.

We now analyze the exceptional cases IB1, IC1, IC3, IC4, and IIIC3, to which all other exceptional cases have been reduced. Write G for $\langle A, B\rangle$. For each of $p = 3$, 11, 19, and 29, the six general cases just considered provide many examples with these values of p for which the conditions of the Main Theorem hold and $P(G) = A_5$ (for example, Theorem 1 of [3] shows that for any triple (α, β, γ) that occurs in the six cases, there is a pair (A, B) in each of $\mathrm{SL}(2, 9)$, $\mathrm{SL}(2, 11)$, $\mathrm{SL}(2, 19)$, or $\mathrm{SL}(2, 29)$ for which $\mathrm{Tr}(A, B) = (\alpha, \beta, \gamma)$, so we can just choose the triple to be (μ_1, μ_1, μ_1) from Case IA7 and achieve that $P(G) = A_5$). So it remains to produce examples for these values of p which satisfy the conditions of the Main Theorem but have $P(G) \neq A_5$.

We begin with case IIIC3, for which we assume that $p = 3$. We have $(\mu_2, 1, 1) \sim (\mu_2, 1, \mu_2 - 1)$. Computing in GAP with $u = Z(9)$, the standard GAP generator for the multiplicative group $\mathbb{F}_9 - \{0\}$, we find that μ_1 can be u or u^3 with corresponding values of μ_2 either u^7 or u^5. But then $\mu_2 - 1$ is either $u^7 - 1 = u^2$ or $u^5 - 1 = u^6$. Since $u^2 = u^3 + u^{-3}$ (or alternatively because $u^2 \in T_4$), a matrix of trace u^2, such as $\begin{pmatrix} u^3 & 0 \\ 0 & u^{-3} \end{pmatrix}$, has order 4 in PSL$(2, 9)$. Since $P(G)$ contains elements of order 4 as well as order 5, $P(G) \not\cong A_5$. The case of $u^6 = u + u^{-1}$ is similar.

For the remaining cases, we have a fixed (odd) value of p and we use u to denote $Z(p)$, the generator used by GAP for the multiplicative group of $\mathbb{F}_p$. We use v for $Z(p^2)^{p-1} \in \mathbb{F}_{p^2}$, for which $v^{(p+1)/2} = -1$.

Assume that $p = 11$, for which $u = 2$, and one of cases IC3 or IC4 occurs. For case IC3, we have $\mu_1 = -3 = u^3$, $(\mu_1, \mu_1, -1) = (u^3, u^3, u^5) \sim (u^3, u^5, u^3) \sim (u^3, u^5, u^9)$. Since $u^9 = v + v^{-1}$, where v has order 12, a matrix of trace u^9 has projective order 6, showing that $P(G) \neq A_5$. For case IC4, $\mu_1 = u^2$, $(\mu_1, \mu_1, 0) = (u^2, u^2, 0) \sim (u^2, u^2, u^4)$. Since $u^4 = v^5 + v^{-5}$, where v^5 has order 12, a matrix of trace u^4 has projective order 6 and $P(G) \neq A_5$.

Assume now that $p = 19$, for which $u = 2$, and case IB1 occurs. We have $\mu_1 = -4 = u^{11}$, and $(u^{11}, u^{11}, -u^{11}) \sim (u^{11}, u^{11}, u^{15})$. Since $u^{15} = u + u^{-1}$, a matrix of trace u^{15} has projective order 9, so $P(G) \neq A_5$.

Finally, we consider $p = 29$, for which $u = 2$ once again, and assume that case IC1 occurs. We have $\mu_1 = -5 = u^8$, $(u^8, u^8, -u^8) \sim (u^8, u^8, u^{24})$, and $u^{24} = v^4 + v^{-4}$ so a matrix of trace u^{24} has order 15.

This completes the proof of the Main Theorem.

As we remarked after the statement of the Main Theorem, in the exceptional cases, it is easy to determine from tr(A), tr(B), and tr(AB) whether or not $P(\langle A, B\rangle) = A_5$. In practice, in the cases when $P(\langle A, B\rangle) \neq A_5$, random applications of the equivalence moves of triples to (α, β, γ) will soon yield an entry that is not in $T_2 \cup T_3 \cup T_5$. But one can tell for certain, as we will illustrate for $p = 3$ (the other cases being similar). Suppose that tr(A), tr(B), tr$(AB) \in T_2 \cup T_3 \cup T_5$ (and at least two are nonzero) and tr$([A, B]) \in \{\mu_1, -\mu_2\}$. Write Tr$(A, B) = (\alpha, \beta, \gamma)$. From proposition 1.1, we know that one of the entries is one of $\pm\mu_1$ or $\pm\mu_2$. Applying equivalences and possibly changing our choice of root of $x^2 - x - 1$, we may assume that $\alpha = \mu_1$. One of β or γ is nonzero, so applying more equivalences we may make (α, β, γ) one of (μ_1, μ_1, γ), (μ_1, μ_2, γ), or $(\mu_1, 1, \gamma)$. If $\gamma \notin T_2 \cup T_3 \cup T_5$, then we already know that $P(\langle A, B\rangle) \neq A_5$. If $\gamma \in T_2 \cup T_3 \cup T_5$, then from the case-by-case analysis of the proof of the "only if" direction of the Main Theorem, (μ_1, β, γ) and the value of $Q(\alpha, \beta, \gamma)$ must now be either as in one of the six general cases IA5, IA7, IIB4, IIB5, IIIA4, or IIIB5, or else as in the special case IIIC3. The proof showed that in the six general cases, $P(\langle A, B\rangle) = A_5$, while in case IIIC3, $P(\langle A, B\rangle) \neq A_5$.

References

1. R. C. Churchill, Two generator subgroups of $\mathrm{SL}(2, \mathbb{C})$ and the hypergeometric, Riemann, and Lamé equations, *J. Symbolic Comput.* 28 (1999) 521–545.
2. GAP: Groups, Algorithms, and Programming, available at the St. Andrews GAP website `http://turnbull.mcs.st-and.ac.uk/~gap/` .
3. A. M. Macbeath, Generators of the linear fractional groups, *Number Theory* (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I. (1969) 14–32.
4. B. H. Neumann and H. Neumann, Zwei Klassencharakteristischer Untergruppen und ihre Factorgruppen, *Math. Nachr.* 4 (1951) 106–125.

Department of Mathematics, University of Oklahoma, Norman, Oklahoma 73019, USA

E-mail address: `dmccullough@math.ou.edu`

URL: `www.math.ou.edu/~dmccullough/`