# SOLVABILITY OF FINITE GROUPS VIA CONDITIONS ON PRODUCTS OF 2-ELEMENTS AND ODD $p$-ELEMENTS 

GIL KAPLAN ${ }^{\boxtimes}$ and DAN LEVY

(Received 14 December 2009)


#### Abstract

We observe that a solvability criterion for finite groups, conjectured by Miller [The product of two or more groups, Trans. Amer. Math. Soc. 12 (1911)] and Hall [A characteristic property of soluble groups, J. London Math. Soc. 12 (1937)] and proved by Thompson [Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. 74(3) (1968)], can be sharpened as follows: a finite group is nonsolvable if and only if it has a nontrivial 2 -element and an odd $p$-element, such that the order of their product is not divisible by either 2 or $p$. We also prove a solvability criterion involving conjugates of odd $p$-elements. Finally, we define, via a condition on products of $p$-elements with $p^{\prime}$-elements, a formation $P_{p, p^{\prime}}$, for each prime $p$. We show that $P_{2,2^{\prime}}$ (which contains the odd-order groups) is properly contained in the solvable formation.


2000 Mathematics subject classification: primaray 20D10; secondary 20E32.
Keywords and phrases: solvable groups, conjugate elements, formations.

## 1. Introduction

Using his result on the classification of minimal simple groups [14] (nonabelian simple groups whose proper subgroups are all solvable), Thompson was able to prove a solvability criterion for finite groups ${ }^{1}$ conjectured, independently, by Miller [11] and by Hall [9].

Criterion 1 [14, Corollary 3]. A group $G$ is nonsolvable if and only if the following condition holds:
Condition A. There exist three nontrivial elements, $a, b, c \in G$, whose orders are coprime in pairs, satisfying $a b c=1_{G}$.

A closer look at Thompson's proof enables one to sharpen this solvability criterion in the following manner.

Criterion 2. A group $G$ is nonsolvable if and only if the following condition holds:

[^0]Condition B. There exist three nontrivial elements, $a, b, c \in G$, such that $a$ is $a$ 2-element, $b$ is a $u$-element where $u$ is an odd prime, and $\operatorname{gcd}(o(c), 2 u)=1$, satisfying $a b c=1_{G}$.

Furthermore, we have the following related observations.
THEOREM 3. Let $G$ be a simple nonabelian group. Then the following condition holds:
Condition C. There exist two odd primes $u \neq v$ and three elements $g_{2}, g_{u}, g_{v} \in G$ such that $o\left(g_{2}\right)=2, o\left(g_{u}\right)=u$ and $o\left(g_{v}\right)=v$, satisfying $g_{2} g_{u} g_{v}=1_{G}$.

THEOREM 4. A group $G$ is solvable if and only if the following condition holds:
Condition D. For any odd prime $p$, any $p$-element $x \in G$ and any 2-element $y \in G$, the group $\left\langle x, x^{y}\right\rangle$ is solvable.

We should mention, in relation to Theorem 4, that a similar, though weaker, solvability criterion was recently, and independently, published in [7, 8]: a finite group $G$ is solvable if and only if every pair of conjugate elements generates a solvable subgroup. This criterion can itself be viewed as a stronger version of another solvability criterion by Thompson [14, Corollary 2]: a finite group $G$ is solvable if and only if every pair of elements generates a solvable subgroup. We note that Flavell [5] proved the last criterion without using the classification of the minimal simple groups.

After proving Criterion 2 and Theorems 3 and 4, we define, for every prime $p$, a class of groups which we denote $P_{p, p^{\prime}}$ (Definition 9 below). We prove that $P_{p, p^{\prime}}$ is a formation, and, using Criterion 2, we show that $P_{p, p^{\prime}}$ is contained in the solvable universe if and only if $p=2$. We give some constructions of $P_{p, p^{\prime}}$ groups and we also show, by way of example, that $P_{2,2^{\prime}}$, which properly contains the formation of odd-order groups, is properly contained in the solvable universe.

## 2. Proofs of Criterion 2 and Theorems 3, 4

Clearly Condition B implies Condition A, so that the sufficiency of Condition B for nonsolvability of $G$ is implied by the sufficiency of Condition A for nonsolvability of $G$ (whose proof is easy and already appears in papers by Miller [11] and Hall [9]). We now prove the necessity of Condition B for nonsolvability. Following Thompson, the proof splits into two steps. First we prove that a minimal counterexample $G$ (a minimal-order nonsolvable group for which Condition B fails) must be minimal simple. Then we show that all minimal simple groups satisfy Condition B and hence there is no counterexample to the claim.
First step. Let $G$ be a minimal counterexample. Since Condition B fails for $G$, it fails for all subgroups of $G$, and hence, by minimality, all proper subgroups of $G$ are solvable. In other words, $G$ is minimal nonsolvable. It is well known that $G$ is minimal nonsolvable if and only if $G / \Phi(G)$ is minimal simple, where $\Phi(G)$ is the Frattini subgroup of $G$. Suppose that $G$ is not minimal simple. Then $\Phi(G)>\left\{1_{G}\right\}$. Let $p$ be a prime dividing $|\Phi(G)|$, and let $N$ be the Sylow $p$-subgroup of $\Phi(G)$. Let $\bar{G}=G / N$.

The nonsolvability of $G$ implies the nonsolvability of $\bar{G}$ and hence, by minimality of $G, \bar{G}$ satisfies Condition B. For any $g \in G$, let $\bar{g}=g N$. By Condition B, there exist nontrivial $a_{1}, b_{1}, c_{1} \in G$ such that $\overline{a_{1}}$ is a 2-element, $\overline{b_{1}}$ is a $u$-element where $u$ is an odd prime, and $\operatorname{gcd}\left(o\left(\overline{c_{1}}\right), 2 u\right)=1$, satisfying $\overline{a_{1}} \overline{b_{1}} \overline{c_{1}}=1 \bar{G}$, and $\overline{a_{1}}, \overline{b_{1}}, \overline{c_{1}}$ are nontrivial. It follows that $a_{1} b_{1} c_{1}=f \in N$. We may assume that $a_{1}$ is a 2-element, and that $b_{1}$ is a $u$-element. Furthermore, we may assume that $\operatorname{gcd}\left(o\left(c_{1}\right), 2 u\right)=1$. We have the following three possibilities.
(1) $\quad p=2$. In this case $\left(f^{-1} a_{1}\right) b_{1} c_{1}=1_{G}$. Note that $f^{-1} a_{1}$ is a nontrivial 2-element since $f \in O_{p}(G)$ and $\overline{a_{1}} \neq 1_{\bar{G}}$. Moreover, $\left(f^{-1} a_{1}\right), b_{1}, c_{1}$ are nontrivial and their orders are coprime in pairs. This contradicts the assumption that Condition B fails in $G$.
(2) $p=u$. In this case $a_{1}\left(b_{1} f^{-1}\right) c_{1}^{\prime}=1_{G}$, where $c_{1}^{\prime}$ is a conjugate of $c_{1}$.
(3) $p \notin\{2, u\}$. In this case $a_{1} b_{1}\left(c_{1} f^{-1}\right)=1_{G}$.

In cases (2) and (3) we get a contradiction using the same type of arguments as in case (1).

Thus the possibility $\Phi(G)>\left\{1_{G}\right\}$ is ruled out, and $G$ must be minimal simple.
Second step. It remains to show that all of the minimal simple groups satisfy Condition B. Instead, we will prove that they satisfy the stronger Condition C.

## Lemma 5. Every minimal simple group satisfies Condition C.

Proof. For any group $G$ let $\chi^{(s)}$ be the $s$ th irreducible character of $G(1 \leq s \leq k)$. Using character theory (see [2, Equation (11.1)]) one can show that a triple ( $g_{2}, g_{u}, g_{v}$ ) such that $g_{2} g_{u} g_{v}=1_{G}$ exists if and only if

$$
\begin{equation*}
\sum_{s=1}^{k} \frac{1}{\chi^{(s)}\left(1_{G}\right)} \chi^{(s)}\left(g_{2}\right) \chi^{(s)}\left(g_{u}\right) \chi^{(s)}\left(g_{v}\right)>0 \tag{1}
\end{equation*}
$$

We now present a choice of $\left(g_{2}, g_{u}, g_{v}\right)$, satisfying Condition C, for each minimal simple group on Thompson's list [14, Corollary 1]. In each case we give the source of the relevant character table and use its notations.
(1) $L_{2}(q), q=2^{p}$ where $p$ is any prime. Character table source: [6, Theorem 4.9]. Here we take $u$ to be a prime divisor of $q-1$ and $v$ a prime divisor of $q+1$. Since $q$ is even, $u$ and $v$ are distinct odd primes. We choose $g_{2}=c$ (an element of order 2), $g_{u}=a^{(q-1) / u}$ and $g=b^{(q+1) / v}$. Since $a$ and $b$ are $L_{2}(q)$ elements of order $q-1$ and $q+1$ respectively, we have $o\left(g_{u}\right)=u, o\left(g_{v}\right)=v$. One can check that

$$
\begin{equation*}
\sum_{s=1}^{k} \frac{1}{\chi^{(s)}\left(1_{G}\right)} \chi^{(s)}\left(g_{2}\right) \chi^{(s)}\left(g_{u}\right) \chi^{(s)}\left(g_{v}\right)=1>0 \tag{2}
\end{equation*}
$$

(2) $L_{2}\left(3^{p}\right), p$ any odd prime.
(3) $L_{2}(p), p$ any prime exceeding 3 such that $p^{2}+1 \equiv 0 \bmod 5$.

We consider cases (2) and (3) together as $L_{2}(q)$ with $q>5$ odd. Character table source: [6, Theorem 4.7]. We have $q=p_{0}^{n}$, where $p_{0}$ is an odd prime, and $n$ a positive integer. Here, $L_{2}(q) \cong S L_{2}(q) / Z\left(S L_{2}(q)\right)$ where $Z\left(S L_{2}(q)\right)=\langle z\rangle$ and $o(z)=2$. In the following, $a$ is an $S L_{2}(q)$ element of order $q-1, b$ is an $S L_{2}(q)$ element of order $q+1$, and $c$ is an $S L_{2}(q)$ element of order $p_{0}$. The tables, and consequently our choice of $u, v$, and $\left(g_{2}, g_{u}, g_{v}\right)$, split according to whether $q \equiv 1 \bmod 4$ or $q \equiv-1 \bmod 4$. Start with $q \equiv 1 \bmod 4$. Since $q-1$ is divisible by 4, we choose an integer $l$ so that $a^{l}$ has order 4 and $g_{2}=\langle z\rangle a^{l}$ has order 2. We choose $g_{u}=\langle z\rangle c\left(o\left(g_{u}\right)=u=p_{0}\right)$. Finally, we choose an integer $r$ and $g=\langle z\rangle b^{r}$ such that $o(g)$ is an odd prime divisor $v$ of $q+1$. Clearly $v \neq p_{0}$. For $q \equiv-1 \bmod 4$, we can choose $r$ so that $o\left(b^{r}\right)=4$, and $g_{2}=\langle z\rangle b^{r}$ has order 2 . We also choose $g_{u}=\langle z\rangle c$ with $o\left(g_{u}\right)=u=p_{0}$, and $g=\langle z\rangle a^{l}$ with $l$ such that $o(g)$ is an odd prime divisor $v$ of $q-1$ and therefore clearly $v \neq p_{0}$. For both $q \equiv 1 \bmod 4$ and $q \equiv-1 \bmod 4$ our choices satisfy Equation (2).
(4) $S z\left(2^{p}\right), p$ any odd prime. Character table source: Suzuki's paper [12]. Set $q=2^{p}$ and $r=2^{(p+1) / 2}$. We take $g_{2}=d\left(d\right.$ is an involution), $g_{u}=a^{l}$ for a suitable $l$ such that $o\left(g_{u}\right)=u$ is a prime divisor of $q-1$ ( $a$ generates a cyclic subgroup of order $q-1$ ), and $g=b^{m}$ such that $o(g)$ is a prime divisor $v$ of $q+r+1$ ( $b$ generates a cyclic subgroup of order $q+r+1$ ). Note that $q-1$ and $q+r+1$ are odd and coprime. This choice satisfies Equation (2).
(5) $L_{3}(3)$. Character table source: GAP's character library [13]. We choose $g_{2}=2 a, g_{u}=3 a, g_{v}=13 a$ (these are representatives of conjugacy classes whose orders are respectively 2, 3, 13). This choice satisfies Equation (2) and thus the second (final) step of the proof is completed.

PRoof of Theorem 3. The theorem follows at once from Lemma 5, once we invoke the result of [1], which states that every simple nonabelian group contains a minimal simple group.

In order to prove Theorem 4, we need the following lemma.
Lemma 6. Let $G$ be a minimal simple group. Then there exists an odd prime $u$, an element $g_{u}$ of order $u$ and an involution $g_{2}$ such that $G=\left\langle g_{u}, g_{u}^{g_{2}}\right\rangle$.
Proof. Since $G$ is minimal simple, there exist, by Lemma 5, two odd primes $u \neq v$ and three elements $g_{2}, g_{u}, g_{v} \in G$ such that $o\left(g_{2}\right)=2, o\left(g_{u}\right)=u$ and $o\left(g_{v}\right)=v$, satisfying $g_{2} g_{u} g_{v}=1_{G}$. Thus $g_{v} \in\left\langle g_{2}, g_{u}\right\rangle$, and, by Criterion 2 (or 1 ), $\left\langle g_{2}, g_{u}\right\rangle$ is not solvable. Since $G$ is minimal simple, $\left\langle g_{2}, g_{u}\right\rangle=G$. Now, we prove that $\left\langle g_{u}, g_{u}^{g_{2}}\right\rangle \unlhd G$. Since $G=\left\langle g_{2}, g_{u}\right\rangle$, it is sufficient to show that $g_{u}^{x},\left(g_{u}^{g_{2}}\right)^{x} \in\left\langle g_{u}, g_{u}^{g_{2}}\right\rangle$ for $x=g_{2}$ and $x=g_{u}$. This is immediate from the fact that $g_{2}$ is an involution. Since $\left\{1_{G}\right\}<\left\langle g_{u}, g_{u}^{g_{2}}\right\rangle \unlhd G$ and $G$ is simple, we get $G=\left\langle g_{u}, g_{u}^{g_{2}}\right\rangle$.

Proof of Theorem 4. If $G$ is solvable then every subgroup of $G$ is solvable. In the other direction, let $G$ be a minimal counterexample to the claim (a minimal-order nonsolvable group for which Condition D holds). Then, since Condition D is inherited by subgroups and quotients, $G$ must be a minimal simple group. By Lemma 6, there
exist an odd prime $p$ and $x, y \in G$ such that $x$ is a $p$-element and $y$ is a 2 -element and $G=\left\langle x, x^{y}\right\rangle$. Hence, by Condition D, $G$ is solvable-a contradiction.

## 3. The $\boldsymbol{P}_{p, p^{\prime}}$ formation

Definition 7. Let $p$ and $q$ be two distinct primes. A group $G$ has the $p, q$-property (equivalently $G \in P_{p, q}$ ) if for every $p$-element $g_{p}$ and every $q$-element $g_{q}$, it holds that $g_{p} g_{q}$ is a $\{p, q\}$-element.

REMARK 8. In the last definition we do not require that $p$ or $q$ are divisors of $|G|$. If, for instance, $p \nmid|G|$ then the $p, q$-property holds trivially in $G$. For later purposes, it is convenient to extend the definition of the $p, q$-property to the case $p=q$ by postulating that every finite group $G$ enjoys the $p, p$-property.
Definition 9. Let $G$ be a group and let $p$ be a prime. We shall say that $G$ satisfies the $p, p^{\prime}$-property if $G \in P_{p, q}$ for every prime $q \neq p$. Equivalently,

$$
P_{p, p^{\prime}} \stackrel{\text { def }}{=} \bigcap_{q \in \mathbb{P}} P_{p, q}
$$

where $\mathbb{P}$ is the set of all primes. We call the $2,2^{\prime}$-property the two-odd property.
Lemma 10. Let $G$ be a group. Let $p$ and $q$ be two primes. If $G \in P_{p, q}$ then every subgroup of $G$ and every quotient group of $G$ are in $P_{p, q}$. If $G=A \times B$ and $A$ and $B$ are in $P_{p, q}$, then $G \in P_{p, q}$.
Proof. Straightforward.
Corollary 11. Let $p$ and $q$ be two primes. Then $P_{p, q}$ is a formation.
Proof. By Lemma 10, $P_{p, q}$ is closed under the operations of taking homomorphic images, subgroups and direct products. Hence it is a formation (see [4, Ch. II, Definition 2.2]).

Corollary 12. Let $p$ be a prime. Then $P_{p, p^{\prime}}$ is a formation.
Proof. $P_{p, p^{\prime}}$ is an intersection of formations (see [4, Ch. II, Remark 1.7]).
Lemma 13. Let $p$ be any prime. If $G$ is nilpotent, then $G \in P_{p, p^{\prime}}$.
Proof. Immediate.
THEOREM 14. Let $G$ be a group. If $G$ has the two-odd property then $G$ is solvable.
Proof. This follows immediately from the definition of the two-odd property and Criterion 2.

Remark 15. Let $p$ be an odd prime. Then there exists $G \in P_{p, p^{\prime}}$ such that $G$ is not solvable. In order to prove this claim it is sufficient to take a nonsolvable group whose
order is not divisible by $p$ (see Remark 8). If $p>5$ take $A_{5}$. If $p=5$ take $L_{3}$ (3). If $p=3$ take $S z(8)$. Note that if $G \in P_{p, p^{\prime}}$ then, by Lemma $10, G \times C_{p} \in P_{p, p^{\prime}}$, where $C_{p}$ is a cyclic group of order $p$. Hence we can easily produce a (trivial) example of a nonsolvable $P_{p, p^{\prime}}$ group whose order is divisible by $p$, where $p$ is an odd prime.

## 4. Examples of $\boldsymbol{P}_{\boldsymbol{p}, \boldsymbol{p}^{\prime}}$ groups

Let $p$ be a prime. All groups whose order is not divisible by $p$ are (trivially) $P_{p, p^{\prime}}$ by Remark 8, and in particular, odd-order groups are two-odd. All groups whose order is divisible by exactly two distinct primes are $P_{p, p^{\prime}}$ for any $p$.

Definition 16. Let $p$ be a prime, $G$ a group and $P$ a Sylow $p$-subgroup of $G$. We shall say that $P$ is $p^{\prime}$-permutable in $G$ if for any prime $q \neq p$ and any Sylow $q$-subgroup $Q$ of $G$ we have $P Q=Q P$.

Note that if a Sylow $p$-subgroup of $G$ is $p^{\prime}$-permutable in $G$, then all Sylow $p$ subgroups of $G$ are $p^{\prime}$-permutable in $G$, and therefore $G \in P_{p, p^{\prime}}$.

Our next result involves Frobenius groups. The following characterization of Frobenius groups best suits our purpose: $G$ is a Frobenius group if and only if there exists $K \unlhd G$ (the Frobenius kernel) such that for every $g \in G-K, \operatorname{gcd}(o(g),|K|)=1$. To see that any group that satisfies this condition is indeed a Frobenius group (the other direction is easy), let $x \in K-\left\{1_{G}\right\}$ and let $y \in C_{G}(x)$. If $y \in G-K$, then, using the assumption and $\operatorname{gcd}(o(x), o(y))=1$, we get $o(x y)=o(x) o(y)$. But $x y \in G-K$, and since $o(x)$ is a nontrivial divisor of $|K|$ we have $\operatorname{gcd}(o(x y),|K|)>1$-a contradiction. Thus $y \in K$ and we get $C_{G}(x) \leq K$ for any $x \in K-\left\{1_{G}\right\}$. This proves that $G$ is a Frobenius group.

THEOREM 17. Let $p$ be a prime. Let $G$ be a Frobenius group, and let $K$ be the Frobenius kernel. If $\bar{G}=G / K \in P_{p, p^{\prime}}$ then $G \in P_{p, p^{\prime}}$ (note that $\bar{G}$ is isomorphic to a Frobenius complement of $G$ ).

Proof. We can assume that $p$ divides $|G|$. Since the Frobenius kernel is always nilpotent, $K \in P_{p, p^{\prime}}$ by Lemma 13. Let $q$ be an arbitrary prime divisor of $|G|$ which is distinct from $p$. Let $a$ be a $p$-element of $G$ and let $b$ be a $q$-element of $G$. We have to show that $a b$ is a $\{p, q\}$-element. We have the following possibilities.
(1) $p$ divides $|K|$. Then $a \in O_{p}(G)$ and so $a b \in O_{p}(G)\langle b\rangle$, which is a $\{p, q\}$ subgroup of $G$.
(2) $\quad q$ divides $|K|$. We argue as in (1).
(3) Both $p$ and $q$ do not divide $|K|$, and hence $a, b \in G-K$. For any $g \in G$ let $\bar{g}=g K$. Since $\bar{G} \in P_{p, p^{\prime}}$ we get that $\overline{a b}$ is a $\{p, q\}$-element. If $a b \in K$ we get $\overline{a b}=\bar{a} \bar{b}=1_{\bar{G}}$ and hence, since $\bar{a}$ is a $p$-element and $\bar{b}$ is a $q$-element with $p \neq q$, $\bar{a}=\bar{b}=1_{\bar{G}}$ and $a, b \in K —$ a contradiction. Hence $a b \in G-K$. This implies $\operatorname{gcd}(o(a b),|K|)=1$. But $o(a b)$ divides $o(\overline{a b})|K|$. Hence $o(a b)=o(\overline{a b})$ which is a $\{p, q\}$-number.

The assumptions of Theorem 17 hold, in particular, for a Frobenius group with a nilpotent Frobenius complement. Thus, such a group is in $P_{p, p^{\prime}}$ for every prime $p$. However, as is shown in Proposition 18 below, such a Frobenius group need not have a Sylow $p$-subgroup which is $p^{\prime}$-permutable in it.

Proposition 18. Let $G$ be a Frobenius group, with a Frobenius kernel $K$ and a Frobenius complement $C$. Let u be a prime divisor of $|G|$. Then a Sylow u-subgroup of $G$ is $u^{\prime}$-permutable in $G$ if and only if either u divides $|K|$ or $|C|$ is a power of $u$.

Proof. Let $U$ be a Sylow $u$-subgroup of $G$. First suppose that $u$ divides $|K|$. Then, since $K$ is nilpotent, we get that $U \unlhd G$ and hence it is $u^{\prime}$-permutable in $G$. Otherwise, $u$ divides $|C|$. If $|C|$ is a power of $u$ then every Sylow $v$-subgroup of $G$, where $v \neq u$ is a prime, is contained $K$ and hence commutes with $U$. Consequently, $U$ is $u^{\prime}$-permutable. Now suppose that $v \neq u$ is a prime dividing $|C|$. Assume to the contrary that $U$ is $u^{\prime}$-permutable in $G$. Let $V$ be any Sylow $v$-subgroup of $G$. Then $U V \leq G$. By [10, 4.1.8(a)], either $U V$ is contained in some Frobenius complement of $G$ or it is itself a Frobenius group with Frobenius kernel $(U V) \cap K$. However $(U V) \cap K=\left\{1_{G}\right\}$ since $U V$ is a $\{u, v\}$-group, so this possibility is ruled out. Thus, $U V$ is contained in some Frobenius complement of $G$ which we can assume, without loss of generality, to be $C$. In particular, $U \leq C$ and $C$ is the unique Frobenius complement containing $U$. It follows that $C$ is the unique Frobenius complement of $G$ containing every Sylow $v$-subgroup of $G$-a contradiction.

Recall [3, Section 2.8] that for a finite field $F$ of order $q, A G L_{1}(F)$ is the group of order $q(q-1)$ which consists of all functions $t_{\alpha, \beta}: F \rightarrow F, \alpha \in F^{\times}, \beta \in F$, defined by $(\zeta) t_{\alpha, \beta}=\alpha \zeta+\beta$ for all $\zeta \in F$. The group $A G L_{1}(F)$ is a Frobenius group whose kernel is isomorphic to the additive group of $F$ and whose Frobenius complement is isomorphic to the multiplicative group $F^{\times}$of $F$ and, in particular, nilpotent. Thus, by Theorem 17, $A G L_{1}(F)$ is in $P_{u, u^{\prime}}$ for any prime $u$. However, if $q-1$ is not a prime power, then, by Proposition 18, a Sylow $u$-subgroup of $A G L_{1}(F)$ is not $u^{\prime}$-permutable in $A G L_{1}(F)$, for any prime $u$ dividing $q-1$.

We conclude our discussion with an example of a family of solvable groups which are not two-odd. Let $q=p^{k}$ where $p$ is a prime, and let $f$ be the Frobenius automorphism $\zeta \longmapsto \zeta^{p}$ of $F$ (note that $o(f)=k$ ). Then $A=\langle f\rangle \leq \operatorname{Sym}(F)$ normalizes $A G L_{1}(F)$, and a suitable semi-direct product $G=A G L_{1}(F) A$ is defined. Clearly $G$ is solvable. The proof of the following proposition uses the product rule, $t_{x, y} t_{z, w}=t_{x z, y z+w}$, of $A G L_{1}(F)$.

Proposition 19. Suppose that $p$ is odd, $k$ is even and $p^{k / 2}+1$ is not a power of 2 . Then $G$ is not two-odd.

Proof. Let $r$ be an odd prime divisor of $p^{k / 2}+1$ (in particular, $r \neq p$ ), and let $\alpha \in F^{\times}$be such that $o_{F^{\times}}(\alpha)=r$ (in particular, $\alpha \neq-1_{F}$ ). Set $g=f^{k / 2}$. Then $o\left(t_{\alpha, 1}\right)=r$ and $o(g)=2$. We shall show that $o\left(g t_{\alpha, 1}\right)=2 p$ which implies that $g t_{\alpha, 1}$ is
not a $\{2, r\}$-element. For every natural number $n$,

$$
\left(g t_{\alpha, 1}\right)^{n}=g^{n}\left(t_{\alpha, 1}\right)^{g^{n-1}}\left(t_{\alpha, 1}\right)^{g^{n-2}} \cdots\left(t_{\alpha, 1}\right)^{g} t_{\alpha, 1}
$$

Since

$$
\left(t_{\alpha, 1}\right)^{g^{n-1}}\left(t_{\alpha, 1}\right)^{g^{n-2}} \cdots\left(t_{\alpha, 1}\right)^{g} t_{\alpha, 1} \in A G L_{1}(F) \quad \text { and } \quad g^{n} \in A
$$

it follows that $\left(g t_{\alpha, 1}\right)^{n}=1_{G}$ only if $g^{n}=1_{G}$. Hence we can assume that $n$ is even, and $\left(g t_{\alpha, 1}\right)^{n}=\left(t_{\alpha, 1}^{g} t_{\alpha, 1}\right)^{n / 2}$, where we have used $o(g)=2$. By routine computation,

$$
t_{\alpha, 1}^{g} t_{\alpha, 1}=t_{\alpha^{p / 2}, 1} t_{\alpha, 1}=t_{\alpha^{k / 2}+1, \alpha+1}=t_{1, \alpha+1}
$$

where we have used the fact that $o_{F^{\times}}(\alpha)=r$ divides $p^{k / 2}+1$. Thus,

$$
\left(g t_{\alpha, 1}\right)^{n}=\left(t_{\alpha, 1}^{g} t_{\alpha, 1}\right)^{n / 2}=\left(t_{1, \alpha+1}\right)^{n / 2}=t_{1, n / 2(\alpha+1)}
$$

Since $\alpha \neq-1_{F}$, we deduce that $o\left(g t_{\alpha, 1}\right)=2 p$ as asserted.

## Acknowledgement

We are grateful to Marcel Herzog for helpful discussions.

## References

[1] M. J. J. Barry and M. B. Ward, 'Simple groups contain minimal simple groups', Publicacions Matemàtiques 41 (1997), 411-415.
[2] M. J. Collins, Representations and Characters of Finite Groups (Cambridge University Press, Cambridge, 1990).
[3] J. D. Dixon and B. Mortimer, Permutation Groups, Graduate Texts in Mathematics, 163 (Springer, Berlin, 1996).
[4] K. Doerk and T. Hawkes, Finite Soluble Groups, de Gruyter Expositions in Mathematics, 4 (de Gruyter, Berlin, 1992).
[5] P. Flavell, 'Finite groups in which every two elements generate a soluble group', Invent. Math. 121 (1995), 279-285.
[6] K. E. Gehles, 'Ordinary characters of finite special linear groups', MSc Dissertation, School of Mathematics and Statistics, University of St. Andrews, 2002. Downloadable from http://www-circa.mcs.st-and.ac.uk/theses.html\#msc.
[7] N. Gordeev, F. Grunewald, B. Kunyavskii and E. Plotkin, 'Baer-Suzuki theorem for the solvable radical of a finite group', Comptes Rendus Acad. Sci. Paris, Ser. I 347 (2009), 217-222.
[8] S. Guest, 'A solvable version of the Baer-Suzuki theorem', Trans. Amer. Math. Soc. in press.
[9] P. Hall, 'A characteristic property of soluble groups', J. London Math. Soc. 12 (1937), 198-200.
[10] H. Kurzweil and B. Stellmacher, The Theory of Finite Groups: An Introduction (Springer, Berlin, 2004).
[11] G. Miller, 'The product of two or more groups', Trans. Amer. Math. Soc. 12 (1911), 326.
[12] M. Suzuki, 'On a class of doubly transitive groups II', Ann. of Math. (2) 79 (1964), 514-589.
[13] The GAP Group, GAP-Groups, Algorithms, and Programming, Version 4.4.12 of 17-Dec-2008 (http://www.gap-system.org).
[14] J. G. Thompson, 'Nonsolvable finite groups all of whose local subgroups are solvable', Bull. Amer. Math. Soc. 74(3) (1968), 383-437.

GIL KAPLAN, The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel e-mail: gilk@mta.ac.il

DAN LEVY, The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel


[^0]:    ${ }^{1}$ All groups considered in this paper are assumed to be finite.

