J. Group Theory, Ahead of Print
DOI 10.1515/JGT.2010.004

Journal of Group Theory

Semi-rational solvable groups

David Chillag and Silvio Dolfi

(Communicated by G. Malle)

Abstract. An element x of a finite group G is called rational if all generators of the group $\langle x\rangle$ are contained in a single conjugacy class. If all elements of G are rational, then G itself is called rational. It was proved by Gow that if G is a rational solvable group then $\pi(G) \subset \{2, 3, 5\}$. We call $x \in G$ semi-rational if all generators of $\langle x\rangle$ are contained in a union of two conjugacy classes. Furthermore, we call $x \in G$ inverse semi-rational if every generator of $\langle x\rangle$ is conjugate to either x or x^{-1}. Then G is called semi-rational (resp. inverse semi-rational) if all elements of G are semi-rational (resp. inverse semi-rational). We show that if G is semi-rational and solvable then $\pi(G) \subset \{2, 3, 5, 7, 13, 17\}$, and if G is inverse semi-rational and solvable then $17 \notin \pi(G)$. If G has odd order, then it is semi-rational if and only if it is inverse semi-rational. In this case we describe the structure of G.

1 Introduction

An element x of a finite group G is called rational if all generators of the group $\langle x\rangle$ are conjugate in G. If all elements of G are rational, then G itself is called rational. It was proved by Gow [3] that if G is a rational solvable group then $\pi(G) \subset \{2, 3, 5\}$. Here we write $\pi(G)$ for $\pi(|G|)$, where $\pi(n)$ is the set of primes dividing the natural number n.

Definition 1. We say that an element $x \in G$ is *semi-rational in G* if there exists a positive integer m_0 such that every generator of $\langle x\rangle$ is conjugate in G to either x or x^{m_0}. We say that an element $x \in G$ is *inverse semi-rational in G* if every generator of $\langle x\rangle$ is conjugate in G to either x or x^{-1}.

We say that a group G is *semi-rational* (resp. *inverse semi-rational*) if every element of G is semi-rational (resp. inverse semi-rational) in G.

Note that semi-rational groups are not necessarily inverse semi-rational. In fact, a Frobenius group of order 78 is a semi-rational, but not an inverse semi-rational group.

Our main result is as follows:

Theorem 2. *Let G be a finite semi-rational solvable group. Then*

$$\pi(G) \subset \{2, 3, 5, 7, 13, 17\}.$$

Furthermore, if G is inverse semi-rational then $17 \notin \pi(G)$.

Observe that each prime $p \in \{2, 3, 5, 7, 13\}$ can actually divide the order of a semi-rational supersolvable group: consider the Frobenius (for $p \neq 2$) group of order $p(p-1)/2$. In fact, we will show (in Section 2) that if G is a semi-rational supersolvable group (or more generally, if G' is nilpotent) then $\pi(G) \subset \{2, 3, 5, 7, 13\}$. As for $p = 17$, we do not know whether it divides the order of any semi-rational solvable group.

If $|G|$ is odd, then G is semi-rational if and only if it is inverse semi-rational (see Remark 13). In this case we can show

Theorem 3. *Let G be a semi-rational group of odd order. Then one of the following holds*:

(1) *G is a Frobenius group of order $3 \cdot 7^a$*;

(2) *$|G| = 7 \cdot 3^b$ and G contains a normal Frobenius subgroup of index 3 with $O_3(G)$ the Frobenius kernel. Moreover $O_3(G)T \in \mathrm{Syl}_3(G)$ for some subgroup T of order 3 and $G/O_3(G)$ is the non-abelian group of order 21*;

(3) *G is a 3-group.*

Examples will be given to show that each of the three cases actually occurs.

Rational groups appear in two problems concerning S_3, the symmetric group of degree 3. One deals with groups G in which elements of the same order are conjugate, and the other with groups G in which elements with the same class size are conjugate. In the former case it was proved by Fitzpatrick [2], and independently by Feit and Seitz [1], that $G \cong S_3$. In the latter case Zhang [11] and Knörr, Lempken and Thielke [7] proved that if G is solvable, then $G \cong S_3$ (it is conjectured that this is true for G non-solvable as well).

Analogous problems for groups G of odd order (in which every element order and every conjugacy class size occurs at least twice) would be the cases in which either every element order or every conjugacy class size occurs exactly twice. Groups satisfying these conditions are semi-rational. In fact in both cases G is the non-abelian group of order 21. This was proved for the conjugacy class size case in [5]. For the element order case, this follows from a more general theorem of Li [8]. In fact, the two results on the groups of order 21 follow easily from Theorem 3.

Finally, we mention that it would be nice to find a characterization of the semi-rational groups in terms of properties of the field of values of their irreducible characters. However, we were unable to do this.

The structure of the paper is as follows. The second section contains some preliminaries and the supersolvable case. The third section is devoted to the proof of Theorem 2. Theorem 3 and some examples can be found in Section 4.

Our notation is standard.

2 Preliminaries

For an element x in the finite group G, we shall write $A(x) = \mathrm{Aut}(\langle x\rangle)$ and $B_G(x) = N_G(\langle x\rangle)/C_G(\langle x\rangle)$. We view $B_G(x)$ as a subgroup of $A(x)$. Observe that x is semi-rational in G if and only if $B_G(x)$ has at most two orbits on the set of generators of $\langle x\rangle$. Also, we denote by $\phi(n)$ the Euler function of the natural number n.

We start with two elementary lemmas.

Lemma 4. *Suppose that the finite group G is (inverse) semi-rational and N is a normal subgroup of G. Then G/N is (inverse) semi-rational.*

Proof. Let $xN \in G/N$ and choose $x_0 \in xN$ of minimal order. Since x_0 is semi-rational in G, there exists a positive integer m_0 such that if $\langle z\rangle = \langle x_0\rangle$, then z is conjugate in G either to x_0 or to $x_0^{m_0}$. We will show that if $yN \in G/N$ with $\langle yN\rangle = \langle xN\rangle$, then yN is conjugate either to xN or to $(xN)^{m_0}$ in G/N.

Since $\langle yN\rangle = \langle xN\rangle$, there exist integers a, b such that $(xN)^a = yN$ and $(yN)^b = xN$. So $x_0^a \in yN$ and $x_0^{ab} \in xN$. By the choice of x_0, we see that $|x_0^{ab}| = |x_0|$ and hence x_0^a must generate $\langle x_0\rangle$. So there exist an element $g \in G$ such that either $(x_0^a)^g = x_0$ or $(x_0^a)^g = x_0^{m_0}$. Hence either $(yN)^{gN} = (x_0^a)^g N = x_0 N = xN$ or $(yN)^{gN} = x_0^{m_0} N = (xN)^{m_0}$. The identical argument with $m_0 = -1$ proves the inverse semi-rational case. □

The complex number field will be denoted by $\mathbb{C}$ and the rational number field by $\mathbb{Q}$. If d is a natural number and ε a primitive dth root of unity, we set $\mathbb{Q}_d = \mathbb{Q}(\varepsilon)$. An element $\alpha \in \mathbb{C}$ is called *quadratic* if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Lemma 5. *Let G be finite group.*

(1) *An element x of order n is semi-rational in G if and only if either x is an involution or $|B_G(x)|$ is divisible by $\frac{1}{2}\phi(n)$.*

(2) *An element x is inverse semi-rational in G if and only if $A(x) = B_G(x)\langle\tau\rangle$, where $\tau \in A(x)$ is the inversion automorphism defined by $\tau(x) = x^{-1}$.*

(3) *If p is a prime of the form $p \equiv 1 \pmod 4$, then a p-element x is inverse semi-rational in G if and only if x is rational in G.*

(4) *If G is abelian, then G is semi-rational if and only if the orders of the elements of G belong to $\{1, 2, 3, 4, 6\}$.*

(5) *If $x \in G$ is semi-rational and $\chi \in \mathrm{Irr}(G)$, then either $\chi(x)$ is quadratic or $\chi(x) \in \mathbb{Q}$.*

Proof. Let $x \in G$ be an element of order n. Set $A = A(x)$ and $B = B_G(x)$. Then A which is isomorphic to the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$, acts regularly and transitively on the set X of generators of $\langle x \rangle$. Then x is semi-rational in G if and only if B has at most two orbits on X. This happens exactly when $|A : B|$ divides 2. When $n > 2$, $\phi(n)$ is even and hence $|A : B|$ divides 2 if and only if $|A|/2 = \frac{1}{2}\phi(n)$ divides $|B|$. This proves (1). Part (2) is obvious.

To see part (3), note that in this case A is cyclic and has order divisible by 4. Hence every subgroup of index 2 in A contains the (unique) involution τ of A. So by (2) we have $A = B$ and x is rational.

If x is an element of order n of the abelian semi-rational group G, then $|B| = 1$ so that $\phi(n) = 1$ or 2. Now part (4) follows.

To see part (5), let d be the order of x and let $H = \mathrm{Gal}(\mathbb{Q}_d/\mathbb{Q})$. If $\sigma \in H$, then $\sigma(\chi(x)) = \chi(x^m)$ for some integer m relatively prime to d. So one verifies that H acts on the set $\Xi = \{\chi(y) \mid \langle y \rangle = \langle x \rangle\}$. However, $|\Xi| \leqslant 2$ because x is semi-rational in G. Hence the subgroup of H that fixes $\chi(x)$ has index at most 2 in H and the Galois correspondence yields (5). □

We recall that if a group G is supersolvable then its commutator subgroup G' is nilpotent. The following result determines the primes that can divide the order of supersolvable semi-rational groups.

Proposition 6. *Let G be a finite group such that G' is nilpotent. If G is semi-rational then $\pi(G) \subseteq \{2, 3, 5, 7, 13\}$, and if G is inverse semi-rational then $\pi(G) \subseteq \{2, 3, 5, 7\}$.*

Proof. We use induction on $|G|$. Let M be a minimal normal subgroup of G. Then M is an elementary abelian p-subgroup for some prime p. Since by Lemma 4 the group G/M is semi-rational, we have $\pi(G/M) \subseteq \{2, 3, 5, 7, 13\}$. If M_1, M_2 are distinct minimal normal subgroups of G, then G is isomorphic to a subgroup of $G/M_1 \times G/M_2$. Then $\pi(G) \subseteq \pi(G/M_1) \cup \pi(G/M_2)$ and we are done.

Hence we can assume that M is the unique minimal normal subgroup of G. As G' is nilpotent, $M \leqslant G'$ and $M \cap Z(G') \neq 1$. Let $x \in M \cap Z(G')$, $x \neq 1$. Then $N_G(\langle x \rangle) \geqslant C_G(x) \geqslant G'$. Hence $B_G(x)$ is isomorphic to a subgroup of some factor group of G/G'. Since x is semi-rational of order p, $B_G(x)$ is cyclic of order $p - 1$ or $(p - 1)/2$. By Lemma 4, any factor group of G/G' is semi-rational and abelian, and by (4) of Lemma 5, the cyclic subgroups of any factor group of G/G' have orders 1, 2, 3, 4, or 6. Thus $p \in \{2, 3, 5, 7, 13\}$ and $\pi(G) = \pi(M) \cup \pi(G/M) \subseteq \{2, 3, 5, 7, 13\}$. If G is an inverse semi-rational and $p = 13$, then by (3) of Lemma 5, x has to be rational and $|B_G(x)| = 12$. However, G/G' has no cyclic section of order 12, a contradiction. So $13 \notin \pi(G)$. This completes the proof. □

Next we have two elementary field-theoretic lemmas.

Lemma 7. *Let $\mathbb{K}$ be a subfield of $\mathbb{C}$. Then the following are equivalent*:

(a) *$\mathbb{K}$ is generated over $\mathbb{Q}$ by quadratic elements*;

(b) $\mathbb{K} \subseteq \mathbb{L}$, *where* $\mathbb{L}$ *is a subfield of* $\mathbb{C}$ *generated over* $\mathbb{Q}$ *by quadratic elements*;

(c) $\mathbb{K}$ *is a Galois extension of* $\mathbb{Q}$ *and* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ *is an elementary abelian* 2*-group.*

Proof. Clearly (a) implies (b). Assume now (b) and let $\mathbb{L} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, with $\alpha_1, \ldots, \alpha_n$ quadratic elements. Write $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. For every i, $\mathbb{F}_i = \mathbb{Q}(\alpha_i)$ is a normal extension of $\mathbb{Q}$, being the splitting field of the minimal polynomial (of degree 2) of α_i over $\mathbb{Q}$. So $\mathbb{L}$ is a Galois extension of $\mathbb{Q}$ and each $N_i = \mathrm{Gal}(\mathbb{L}/\mathbb{F}_i)$ is a normal subgroup of index 2 in G. Observe that $\bigcap_{i=1}^n N_i = 1$, since $\mathbb{L}$ is generated by $\alpha_1, \ldots, \alpha_n$ over $\mathbb{Q}$. Thus, $G = G/\bigcap_{i=1}^n N_i$ is isomorphic to a subgroup of the direct product $\prod_{i=1}^n G/N_i$ and hence G is an elementary abelian 2-group. Let M be the subgroup of G consisting of the automorphisms that fix the elements of $\mathbb{K}$. Then M is normal in G and hence $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$. Moreover, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq G/M$ is an elementary abelian 2-group. So we have (c).

Finally, we assume (c) and prove (a). Let $M_1, \ldots, M_k$ be the maximal subgroups of $H = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. As H is a 2-group, we have $|H : M_i| = 2$ for every i. Therefore for every i, the fixed field $\mathbb{F}_i$ of M_i on $\mathbb{K}$ has degree 2 over $\mathbb{Q}$, so $\mathbb{F}_i = \mathbb{Q}(\alpha_i)$ for a quadratic element $\alpha_i \in \mathbb{C}$. Let $\mathbb{E} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. Since H is elementary abelian, we have that $\bigcap_{i=1}^k M_i = 1$. Now, if $\phi \in \mathrm{Gal}(\mathbb{K}/\mathbb{E})$, then $\phi \in \mathrm{Gal}(\mathbb{K}/\mathbb{F}_i) = M_i$ for all i and hence $\phi = \mathrm{id}_{\mathbb{K}}$. Thus, by the Galois correspondence, $\mathbb{K} = \mathbb{E}$. □

Lemma 8. *Let* $\mathbb{K}$ *be a subfield of* $\mathbb{C}$ *generated over* $\mathbb{Q}$ *by quadratic elements and let* d *be a positive integer. Then* $[\mathbb{K} \cap \mathbb{Q}_d : \mathbb{Q}]$ *divides* $2^{|\pi(d)|}$ *if* d *is odd and it divides* $2^{|\pi(d)|+1}$ *if* d *is even.*

Proof. Given a positive integer n, we denote by $U(n)$ the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$. Let $d = q_1^{a_1} \ldots q_m^{a_m}$ be the prime power decomposition of d. Then $\Delta = \mathrm{Gal}(\mathbb{Q}_d/\mathbb{Q}) \simeq U(d) \simeq \prod_{i=1}^m U(q_i^{a_i})$. For a prime q and a positive integer a, the group $U(q^a)$ is a cyclic group (of order $q^{a-1}(q-1)$) if either $q \neq 2$ or if $q = 2$ and $a \leqslant 2$; otherwise it is of type $C_{2^{a-2}} \times C_2$. It follows that the largest factor group of exponent 2 of Δ has order 2^m if d is odd, and order at most 2^{m+1} if d is even. Now, $\mathrm{Gal}(\mathbb{K} \cap \mathbb{Q}_d/\mathbb{Q})$ is a factor group of both Δ and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Recalling that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is an elementary abelian 2-group by Lemma 7, we conclude that $[\mathbb{K} \cap \mathbb{Q}_d : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{K} \cap \mathbb{Q}_d/\mathbb{Q})|$ divides $2^{|\pi(d)|}$ if d is odd and it divides $2^{|\pi(d)|+1}$ if d is even. □

Another simple fact that we need is the following result:

Lemma 9. *Let* $G = \langle x, y \mid x^{2^{n-1}} = 1,\ y^2 = x^{2^{n-2}},\ y^{-1}xy = x^{-1} \rangle$ *be the quaternion group of order* 2^n*, where* $n \geqslant 4$*. Then the following assertions hold.*

(1) *Every subgroup of* G *is either a cyclic group or a quaternion group.*

(2) *All elements in* $G - \langle x \rangle$ *are of order* 4*. The group* G *has a unique cyclic subgroup of order* 2^m*, for every* m *such that* $3 \leqslant m < n$*.*

(3) *Every normal subgroup of index bigger than* 2 *in* G *is cyclic.*

Proof. Claim (1) and the first part of Claim (2) are well known. So, if $T \leqslant G$ is a cyclic group of order bigger than 4, then $T \leqslant \langle x \rangle$, and the second part of Claim (2) follows. Claim (3) is [9, Proposition 9.10 (ii)]. □

3 Solvable semi-rational groups

The proof of Theorem 2 uses methods developed in [3] and [10]. We need the following definition.

Definition 10. Let H be a finite group and V an H-module over a finite field $\mathbb{F}$. Let k be a divisor of $|\mathbb{F}^\times|$. We say that the action of H on V (or, for brevity, that V) has the *k-eigenvalue property* if for every $\mu \in \mathbb{F}^\times$ of order k and for every $v \in V$, there exists some $g \in G$ such that $vg = \mu v$.

Clearly, in the above definition 'for every μ of order k' can be replaced by 'for some μ of order k', since the multiplicative group $\mathbb{F}^\times$ is cyclic. We also remark that if the action of H on V has the k-eigenvalue property, than it also has the h-eigenvalue property for every divisor h of k.

Remark 11. If the action of H on V is Frobenius (that is, if $C_V(h) = \{0\}$ for every $h \in H$, $h \neq 1$) and $\mu \in \mathbb{F}^\times$ has order k, then every $g \in G$ such that $vg = \mu v$ must be of order k. This is since $vg^k = v$ and hence, by the Frobenius action, $|g|$ divides k. On the other hand, $vg^i = \mu^i v \neq v$ for $0 < i < k$, since $\mu^i \neq 1$. Thus $|g| = k$.

Lemma 12. *Let H be a finite solvable group and V be an H-module over a finite field $\mathbb{F}$ of characteristic p, where p does not divide $|H|$. Assume that the action of H on V is Frobenius. Write $n = \dim_{\mathbb{F}}(V)$. Let φ be the Brauer character afforded by V and let $\mathbb{K} = \mathbb{Q}(\varphi)$ be the field of values of φ. Let $g \in H$ be an element of order d and $m = [\mathbb{Q}_d : \mathbb{Q}_d \cap \mathbb{K}]$. Then*

(a) *m divides n.*

Assume further that d divides $|\mathbb{F}^\times|$.

(b) *If μ is an element of order d of $\mathbb{F}^\times$, then the dimension (over $\mathbb{F}$) of the μ-eigenspace of g in V is at most n/m.*

(c) *Suppose further that the action of H on V has the k-eigenvalue property. If d is a prime divisor of k, and $d \geqslant 5$, then $\mathbb{K}$ contains a primitive d-th root of unity.*

Proof. (a), (b) and (c) come from [10, Lemmas (4.3), (4.6) and (4.10)] respectively. □

Proof of Theorem 2. We use induction on $|G|$. Using Lemma 4 and the usual subdirect product argument (see for example the first paragraph of the proof of Proposition 6), we can assume that G has a unique minimal normal subgroup V. Write $|V| = p^n$, where p is a prime. Then, working toward a contradiction, we can assume that $p \notin \pi = \{2, 3, 5, 7, 13\}$ (also $p \neq 17$ if G is not inverse semi-rational), while

$\pi(G/V) \subseteq \pi \cup \{17\}$ (and even $\pi(G/V) \subseteq \pi$ if G is inverse semi-rational). In any case, $(|V|, |G:V|) = 1$, so there is a complement H of V in G. As V is the only minimal normal subgroup of G, we see that V is a faithful irreducible H-module.

Let $k = (p-1)/2$ and v be an element in V. Since v is semi-rational in G, we know that $B_G(v) = N_G(\langle v\rangle)/C_G(\langle v\rangle)$ is a subgroup of index at most 2 of the automorphism group $A(v) = \mathrm{Aut}(\langle v\rangle)$. Using additive notation in V, we can identify $A(v)$ with the multiplicative group of the field $\mathbb{F} = \mathrm{GF}(p)$. Let μ_1 an element of order $p-1$ of $\mathbb{F}^\times$ and $\mu = (\mu_1)^2$. Then μ has order k and $B_G(v)$ can be identified with the either $\langle\mu\rangle$ or $\langle\mu_1\rangle$. Hence there exists an element $g \in G$ such that $vg = \mu v$ (where we are writing vg instead of v^g, as we are using the additive notation in V) and, as $V \leqslant C_G(v)$, we can in fact choose g to be in H. Therefore, the action of H on V has the k-eigenvalue property. By (3) of Lemma 5, the same is true for $k = p-1$, if G is inverse semi-rational and $p \equiv 1 \pmod 4$.

We denote by φ the Brauer character of H afforded by V and by $\mathbb{K} = \mathbb{Q}(\varphi)$ its field of values. As $|H|$ is coprime to p, then φ is in fact an ordinary character of H. So φ is a sum of irreducible characters of H and hence $\mathbb{K} \subseteq \mathbb{L}$, where $\mathbb{L}$ is the field generated over $\mathbb{Q}$ by the set $Y = \{\chi(h) \mid \chi \in \mathrm{Irr}(H), h \in H\}$. Since $H \simeq G/V$ is semi-rational, then for every $\alpha \in Y$ either α is quadratic or $\alpha \in \mathbb{Q}$ by (5) of Lemma 5. Hence, by Lemma 7, the field $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$ and $\mathbb{K}$ is generated over $\mathbb{Q}$ by quadratic elements.

Now, if M_0 is a maximal element (with respect to inclusion) of the family $\{C_H(v) : v \in V, v \neq 0\}$, $N_0 = N_H(M_0)$ and $W_0 = C_V(M)$, then by [10, Lemma (4.1)] the action of N_0/M_0 on W_0 is Frobenius, it has the k-eigenvalue property and, if φ_0 is the Brauer character of N_0/M_0 afforded by W_0, the field of values $\mathbb{K}_0 = \mathbb{Q}(\varphi_0)$ is contained in $\mathbb{K}$. Hence, by changing notation, we can assume that the action of H on V is Frobenius, with the k-eigenvalue property and that, again by Lemma 7, the field $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$, generated by quadratic elements. (But observe that the new $G = V \rtimes H$ is not necessarily semi-rational any more.) Also, clearly $\pi(H) \subseteq \pi \cup \{17\}$ (resp. $\pi(H) \subseteq \pi$ if G is inverse semi-rational). We now proceed in a number of steps.

(I) $p - 1 = 2^a 3^b$, for some non-negative integers a, b.

If $q \geqslant 5$ is a prime divisor of $p-1$, then q also divides k. So by Remark 11, the subgroup H has an element of order q and by Lemma 12(c), $\mathbb{K}$ contains a primitive qth root of unity, i.e. $\mathbb{Q}_q \leqslant \mathbb{K}$. But this implies that $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q})$, which is (a cyclic group) of exponent $q - 1 \geqslant 4$, is a factor group of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, which is of exponent 2, a contradiction.

(II) $b \leqslant 1$.

Assume that $b \geqslant 2$, so that $k = (p-1)/2$ is divisible by 9. We know that the action of H on V is a Frobenius action, so the Sylow subgroups of H are either cyclic or quaternion groups. Using the fact that H is solvable, one can deduce (see [10, Lemma (3.4)]) that there exists a normal subgroup M of H, with $|H:M|$ not divisible by 3, and such that M has a normal 3-complement $K = C \times Q$ where C is cyclic of odd order and Q is either a cyclic 2-group or $Q \simeq Q_8$. Let $T \in \mathrm{Syl}_3(M)$. Then $M = (C \times Q)T$.

Since 9 divides k, the action of H on V has in particular the 9-eigenvalue property. Fix an element μ of order 9 in $\mathbb{F}^\times$. Then, for every $v \in V$, there exists some $h \in H$ such that $vh = \mu v$. By Remark 11, we have $|h| = 9$.

Let $X = \{x \in H : |x| = 9\}$ and, for $x \in X$, write

$$W_x = \{v \in V : vx = \mu v\},$$

the μ-eigenspace of x in V. By the previous paragraph,

$$V = \bigcup_{x \in X} W_x. \tag{1}$$

Write $n = \dim_{\mathbb{F}}(V)$ and $m = [\mathbb{Q}_9 : \mathbb{Q}_9 \cap \mathbb{K}]$. By Lemma 12(a), (b), we know that m divides n and that $\dim_{\mathbb{F}}(W_x) \leqslant n/m$. Further $[\mathbb{Q}_9 \cap \mathbb{K} : \mathbb{Q}] \leqslant 2$ by Lemma 8, so $m = 3$ or $m = 6$. Hence 3 divides n and $\dim_{\mathbb{F}}(W_x) \leqslant n/3$ for all $x \in X$.

We are now going to bound $|X|$. Clearly $|X| \leqslant 6n_3(M)$, where $n_3(M)$ is the number of Sylow 3-subgroups of M (and hence of H). Observe that if Q is cyclic, then T centralizes Q, because in this case $\mathrm{Aut}(Q)$ is a 2-group. If $Q \simeq Q_8$, in any case T centralizes the (unique) involution in Q. Recall now that $\pi(C) \subseteq \{5, 7, 13, 17\}$ and write $C = C_0 \times D$, where C_0 is the Hall $\{5, 17\}$-subgroup and D is the Hall $\{7, 13\}$-subgroup of C. If $q \in \{5, 17\}$, then the automorphism group of a cyclic q-group has order coprime to 3. Thus T centralizes C_0. Hence

$$n_3(M) = |M : N_M(T)| = |K : C_K(T)|$$

divides $4d$, where $d = |D|$. Therefore,

$$|X| \leqslant 24d.$$

Finally, we need to relate d to the dimensions of the eigenspaces W_x. Since D is cyclic, by Lemma 12(a) we get that $e := [\mathbb{Q}_d : \mathbb{Q}_d \cap \mathbb{K}]$ divides n. Now Lemma 8 implies that

$$e = \frac{[\mathbb{Q}_d : \mathbb{Q}]}{[\mathbb{Q}_d \cap \mathbb{K} : \mathbb{Q}]} = z \cdot \frac{\phi(d)}{4}$$

for some positive integer z. We know that $n = 3f$ for some positive integer f. Hence $\phi(d)/12$ divides f. We also know that $\dim(W_x) \leqslant f$ for every $x \in X$. Since by (1) we have $|V| \leqslant \sum_{x \in X} |W_x|$, we get $p^{3f} \leqslant |X| p^f \leqslant 24dp^f$, so $p^{2f} \leqslant 24d$. Recalling that $p \geqslant 19$ (as 9 divides $p - 1$), we conclude immediately that $d \geqslant 16$ and hence $d \geqslant 49$, because $\pi(d) \subseteq \{7, 13\}$. Further, we have $\phi(d) \geqslant (72/91)d \geqslant (7/9)d$ and we conclude that $2f \geqslant \phi(d)/6 \geqslant \beta d$, where $\beta = 7/54$.

So

$$p^{\beta d} \leqslant p^{2f} \leqslant 24d.$$

But it is easily verified that $p^{\beta d} > 24d$ for every $p \geqslant 19$ and $d \geqslant 49$, a contradiction. So (II) is proved.

(III) $a \leqslant 4$, and $a \leqslant 3$ if G is inverse semi-rational.

Assume that $a \geqslant 5$ or $a \geqslant 4$ if G is inverse semi-rational. In each case, the action of H on V has the 16-eigenvalue property. In particular, it follows that $\exp(S) \geqslant 16$, where S is a Sylow 2-subgroup of H.

Assume first that S is non-cyclic. (Here the argument is similar to the first part of Step 5 in [3, Lemma 6].) Then S is a generalized quaternion group of order 2^n, where $n \geqslant 5$ as $\exp(S) \geqslant 16$.

Let $K = O_2(H)$; note that K is normal in H and that $K \leqslant S$. Lemma (3.3) of [10] implies that $|S : K| = 1, 2$, or 4. So $|K| = 2^k$, with $k \geqslant 3$, and K is either cyclic or a quaternion group. Observe that if $k = 3$, then K is cyclic by (3) of Lemma 9. Thus, by Lemma 9, in any case K contains a unique cyclic subgroup T of order 8, which must be equal to the unique cyclic subgroup of order 8 of every Sylow 2-subgroup of H. Hence T is the only cyclic subgroup of order 8 of H. Moreover, T lies in the unique cyclic subgroup of index 2 of S, and Lemma 9 implies that T cannot contain all elements of S of order 4.

Fix an element v of order 8 in $\mathbb{F}^\times$ and $v \in V, v \neq 0$. Let now h be any element of order 4 of S. Then the eigenvalues of h on V lie in $\langle v \rangle$ and there is an integer i such that $vh = v^i v$. Further, as V has the 8-eigenvalue property, there exists a $g \in H$ such that $vg = vv$. By Remark 11, it follows that $|g| = 8$ and hence $\langle g \rangle = T$. As $v(g^i h^{-1}) = v$ and $v \neq 0$, by Frobenius action we get that $h = g^i \in T$. Thus, every element of order 4 of S belongs to T, a contradiction.

We can hence assume that the Sylow 2-subgroups of H are cyclic. So all Sylow subgroups of H are cyclic and hence H is metacyclic. It easily follows that $M = O^{2'}(H)$ has a cyclic normal 2-complement D. Fix an element μ of order 16 in $\mathbb{F}^\times$. For $x \in H$, denote by W_x the μ-eigenspace of x on V. Since by Remark 11 the subgroup H has elements of order 16, by Lemma 12(a) we conclude that $r = [\mathbb{Q}_{16} : \mathbb{Q}_{16} \cap \mathbb{K}] = [\mathbb{Q}_{16} : \mathbb{Q}]/[\mathbb{Q}_{16} \cap \mathbb{K} : \mathbb{Q}]$ divides $n = \dim_{\mathbb{F}}(V)$. Since by Lemma 8 we have $[\mathbb{Q}_{16} \cap \mathbb{K} : \mathbb{Q}] \leqslant 4$, it follows that 2 divides r and hence $n = 2f$ for some positive integer f. Also, by Lemma 12(b), we have $\dim_{\mathbb{F}}(W_x) \leqslant n/r \leqslant f$.

Denote now by X the set of all elements of order 16 of H. Clearly $X \subseteq M$. By Remark 11, we see that $W_x \neq \varnothing$ only if $x \in X$. By the 16-eigenvalue property, we see that that $V = \bigcup_{x \in X} W_x$. Since $|W_x| \leqslant p^f$ for every $x \in X$, we get

$$p^{2f} \leqslant |X| p^f. \tag{2}$$

Now the number of Sylow 2-subgroups of M is at most $|D|$, and each of these Sylow 2-subgroups is cyclic. Therefore $|X| \leqslant 8|D|$, and we obtain

$$p^f \leqslant 8d, \tag{3}$$

where $d = |D|$. Let c be any divisor of $|D|$ and C be a subgroup of order c of D. Because C is cyclic, Lemma 12(a) yields that $m = [\mathbb{Q}_c : \mathbb{Q}_c \cap \mathbb{K}]$ divides $n = 2f$. Now

$$m = [\mathbb{Q}_c : \mathbb{Q}_c \cap \mathbb{K}] = \frac{[\mathbb{Q}_c : \mathbb{Q}]}{[\mathbb{Q}_c \cap \mathbb{K} : \mathbb{Q}]} = \frac{\phi(c)}{2^t}$$

where $t \leqslant |\pi(c)|$ by Lemma 8. Hence for every divisor c of d we have

$$\frac{\phi(c)}{2^{|\pi(c)|}} \quad \text{divides} \quad 2f. \tag{4}$$

In particular, $\phi(d)/2^{|\pi(d)|}$ divides $2f$ and, since $\pi(d) \subseteq \rho := \{3, 5, 7, 13, 17\}$, we get $f \geqslant \phi(d)/2^6$. Moreover, $\phi(d) \geqslant \alpha d$, where $\alpha = \prod_{q \in \rho}(q-1)/q > 3/8$. Hence, from (3), we obtain

$$p^{\beta d} \leqslant 8d, \tag{5}$$

where $\beta = 3/2^9$.

Assume first that $p \neq 17$. Since $p = 2^a 3^b + 1$ is a prime, with $a \geqslant 4$ and $b \in \{0, 1\}$, then $p \geqslant 97$. But then (5) implies that $d \leqslant 290$ and hence (3) yields $f = 1$, that is, $n = 2$. Now, recalling (4) we see that 7, 13 and 17 do not divide d and that, if $d = 3^u 5^v$, then also $0 \leqslant u, v \leqslant 1$. Thus (3) yields that $p = 97$ and $d = 15$. Hence H is a subgroup of $\mathrm{GL}(2, 97)$. But $|\mathrm{GL}(2, 97)|$ is not divisible by 5, a contradiction.

Finally, assume that $p = 17$ and G is inverse semi-rational. Now (5) yields that $d < 500$ and hence, by (3), we get $f \leqslant 2$. Thus, by applying (4) we see that 3^2, 5^2, 7 and 13 do not divide d, so d divides 15. Now (3) implies that $f = 1$. Therefore, $n = 2$ and H is a subgroup of $\mathrm{GL}(2, 17)$. In particular, 5 does not divide $|H|$ and hence d divides 3.

Let $X_0 = \{x \in X : W_x \neq \{0\}\}$ be the set of the elements of H which have some non-zero μ-eigenvector in V. If $x \in X_0$, then $T = \langle x \rangle$ is the subgroup of order 16 of some Sylow 2-subgroup S of H. Also $\dim_{\mathbb{F}}(W_x) \leqslant n/r \leqslant f = 1$, forcing $\dim_{\mathbb{F}}(W_x) = 1$. We claim that $|T \cap X_0| = 2$.

In fact, since $\mu \in \mathbb{F} = \mathrm{GF}(17)$ is an eigenvalue of $x \in \mathrm{Aut}(V) = \mathrm{GL}(2, 17)$, then both eigenvalues of x belong to $\mathbb{F}$. Note that they are distinct. Otherwise x is central in H, so $\langle x \rangle$ is normal in H and hence $X \subseteq \langle x \rangle$. But then $|X| \leqslant 8$, against (2). Denote by λ the eigenvalue $\neq \mu$ of x on V. Since the action of $\langle x \rangle$ on V is Frobenius, λ is an element of order 16 in $\mathbb{F}^\times$; so $\lambda = \mu^v$, for some odd v with $1 \leqslant v \leqslant 16$. Let u be the positive integer such that $uv \equiv 1 \pmod{16}$ and $1 \leqslant u \leqslant 16$. If $y \in \langle x \rangle$, say $y = x^h$ for some $1 \leqslant h \leqslant 16$, then the eigenvalues of y on V are μ^h and μ^{vh}. We conclude that $T \cap X_0 = \{x, x^u\}$, because for $2 \leqslant h \leqslant 16$ we have $\mu^h \neq \mu$ and $\mu^{vh} = \mu$ if and only if $h = u$.

It follows that $|X_0|$ is at most twice the number of Sylow 2-subgroups of H and hence $|X_0| \leqslant 2d$. Observe now that V is covered by the one-dimensional subspaces $\{W_x : x \in X_0\}$. This yields $|X_0| \geqslant 18 > 2d$, the final contradiction. □

4 Semi-rational groups of odd order

We start with a remark.

Remark 13. If $|G|$ is odd, then G is semi-rational if and only if it is inverse semi-rational. Assume that G is semi-rational. Then, for every element $x \in G$, the automorphism group $B_G(x)$ induced by G on $\langle x \rangle$ has at most two orbits on the set of the generators of $\langle x \rangle$. But in a group of odd order no non-identity element is conjugate to its inverse. Thus, every generator of $\langle x \rangle$ is conjugate either to x or to x^{-1}. Hence, if G is semi-rational, it is inverse semi-rational. The converse is clear.

We now prove Theorem 3, which describes the semi-rational groups of odd order. In the proof we could have used Higman's result describing the solvable groups with just prime-power order elements (see [4, Theorem 1]). We chose, instead, to present a self-contained argument.

Proof of Theorem 3. We use induction on $|G|$. Let $y \in G$ an element of order $n \neq 1$. Since y cannot be rational, Lemma 5 implies that $|B_G(y)| = \frac{1}{2}\phi(n)$. Write $n = p_1^{a_1} \dots p_l^{a_l}$ where $p_1, \dots, p_l$ are distinct primes and $a_1, \dots, a_l$ positive integers. Then $\frac{1}{2}\phi(n) = \left(\frac{1}{2}(p_1 - 1)\right)(p_2 - 1)u$ for some u. Since $\frac{1}{2}\phi(n)$ is odd, we conclude that $l = 1$. So the order of every element of G is a prime power and two elements of relatively prime order will never commute.

Let r be the smallest prime dividing $|g|$ an d an element of order r. Then $\frac{1}{2}\phi(r) = \frac{1}{2}(r - 1)$ divides $|G|$ and is smaller than r. Thus $\frac{1}{2}(r - 1) = 1$ and $r = 3$. If $|G|$ has only one prime divisor, then G is a 3-group and conclusion (3) holds. So we may assume that $|G|$ is divisible by at least two distinct primes.

Let N be a minimal normal subgroup of G. As G is solvable by the Feit–Thompson theorem, N is an elementary abelian p-subgroup, for some prime p. Let Q be a p'-Hall subgroup of G. Then in the group QN no element of Q will commute with elements of N. So NQ is a Frobenius group with kernel N and Q a complement. Consequently $Z(Q) \neq 1$ (see [6, Satz 8.18, p. 506]). Let $a \in Z(Q) - \{1\}$. Then a is a q-element for some prime q, and it will commute with an element of prime order for every prime dividing $|Q|$. This forces Q to be a q-group. Thus G is a $\{p, q\}$-group.

As Q is a Frobenius complement, it is cyclic, generated, say, by b. Let $|b| = q^v$, where v is a positive integer. Clearly $Q \subset C_G(b)$ and so q cannot divide $|N_G(\langle b \rangle)/C_G(\langle b \rangle)| = \frac{1}{2}\phi(q^v) = q^{v-1}\left(\frac{1}{2}(q - 1)\right)$. Thus $v = 1$ and $|Q| = q$, and so $|G| = p^w q$ for some positive integer w. Let P be a Sylow p-subgroup of G.

Assume first that $N_G(Q) = Q$. Then $N_G(Q) = Q = C_G(Q)$ and by a theorem of Burnside (see [6, Satz 2.6, p. 416]) G has a normal q-complement, which must be P. Moreover,

$$\left|\frac{N_G(\langle b \rangle)}{C_G(\langle b \rangle)}\right| = \left|\frac{N_G(Q)}{C_G(Q)}\right| = 1 = \frac{1}{2}\phi(q) = \frac{q - 1}{2}.$$

So $q = 3$. Let $z \in P$ be an element of order p. Then $\frac{1}{2}(p-1)$ divides $|G| = 3p^w$ and $\left(\frac{1}{2}(p-1), p\right) = 1$. Hence $\frac{1}{2}(p-1) = 3$ and $p = 7$. As Q acts on the normal 7-subgroup P with no fixed points, conclusion (1) holds.

Thus we may assume that $N_G(Q) > Q$. As no q-element commute with a p-element, $C_G(Q) = Q$ and so $|N_G(Q)/C_G(Q)| = \frac{1}{2}(q-1) > 1$, so $q \neq 3$. It follows that $p = 3$. Clearly $N \leqslant O_3(G)$. By the Schur–Zassenhaus theorem, $N_G(Q) = QT$, where T is a non-trivial 3-group. As G contains no element of order $3q$, T acts on Q fixed-point freely. Hence QT is a Frobenius group with kernel Q and a complement T. It follows that T is cyclic.

Next $N_G(Q) \cap O_3(G) \lhd N_G(Q)$ and $Q \lhd N_G(Q)$ with $(N_G(Q) \cap O_3(G)) \cap Q = 1$ ($N_G(Q) \cap O_3(G)$ being a 3-group and Q a q-group). Again, since G contains no element of order $3q$ we get that $N_G(Q) \cap O_3(G) = 1$. In particular $T \cap O_3(G) = 1$.

Note that $|G/O_3(G)| = 3^w q/|O_3(G)|$ is divisible by $3q$ and $O_3(G/O_3(G)) = 1$. By induction $q = 7$ and $G/O_3(G)$ is the Frobenius group of order 21. Observe that $QO_3(G)/O_3(G)$ is a normal Sylow 7-subgroup of $G/O_3(G)$. Hence $QO_3(G)$ is a normal subgroup of index 3 in G, and since Q acts with no fixed points on $O_3(G)$, it is a Frobenius group. The Frattini argument implies that

$$G = N_G(Q)QO_3(G) = TQO_3(G) = (TO_3(G))Q,$$

with any two of the three subgroups intersecting trivially. Thus $TO_3(G)$ is a Sylow 3-subgroup of G. So conclusion (2) holds. □

Clearly the non-abelian group of order 21 is an example of conclusion (1) of Theorem 3. Every 3-group of exponent 3 is trivially an example of conclusion (3). We now present non-trivial examples of conclusions (1) and (2) and an example of exponent 9 of conclusion (3).

Example 1. Let P be an extraspecial group of order 7^3 and exponent 7. Let a, b be generators of P (so $a^7 = b^7 = 1$ and $1 \neq c = [a, b] \in Z(P)$). Consider a group $A = \langle \alpha \rangle$ of order 3 acting on P by $a^\alpha = a^2$ and $b^\alpha = b^2$. Then $c^\alpha = [a^2, b^2] = c^4$. Hence the action of A on P is Frobenius, since it fixes no non-trivial element both in $Z = Z(P)$ and in P/Z. Let $G = P \rtimes A$. We show that G is a semi-rational group. It is enough to prove that every element in P is semi-rational in G. This is clear for $x \in Z$, since A induces an automorphism of order 3 on Z. Now let $x \in P \backslash Z$. Write $V = \langle x \rangle Z$. Since V is a maximal subgroup of P, we have $V \trianglelefteq P$. Now $\langle x \rangle$ is not normal in P, because otherwise $\langle x \rangle \cap Z \neq 1$ implies that $x \in Z$, and hence $N_G(\langle x \rangle) = V$. So P/V acts transitively on the 1-dimensional subspaces of V not equal to $\langle c \rangle$.

Observe now that $A \leqslant N_G(V)$, since A fixes all linear subspaces of P/Z and hence also $\langle x \rangle Z/Z = V/Z$. As A normalizes $\langle c \rangle$, by Maschke's theorem $V = \langle c \rangle \times \langle y \rangle$ for some $y \in V$ such that $A \leqslant N_G(\langle y \rangle)$. By the previous paragraph, there exists $z \in P$ such that $\langle y \rangle^z = \langle x \rangle$. Hence $B := A^{z^{-1}} \leqslant N_G(\langle x \rangle)$. Also we have $B \cap C_G(\langle x \rangle) = 1$ because the action of B on P, as well as the action of A is Frobe-

nius. It follows that B is isomorphic to a subgroup of $N_G(\langle x\rangle)/C_G(\langle x\rangle)$ and hence, as $|x| = 7$ and $|B| = 3$, x is semi-rational in G.

Example 2. Let $\mathbb{F} = \mathrm{GF}(3^6)$ and H be the subgroup of order 7 of the multiplicative group of $\mathbb{F}^\times$. Consider the following subgroup of the affine semilinear group $A\Gamma(\mathbb{F})$:

$$G = \left\{ \begin{pmatrix} x \\ ax^\sigma + b \end{pmatrix} : x, b \in \mathbb{F}, a \in H, \sigma \in \mathrm{Gal}(\mathbb{F}/\mathrm{GF}(3)) \right\}.$$

Then G is a semi-rational group, $|G| = 3^7 \cdot 7$ and G has a normal Frobenius subgroup K of index 3 in G; the Frobenius kernel of K is $F = O_3(G)$ (an elementary abelian group of order 3^6) and G/F is a Frobenius group of order 21. To prove that G is semi-rational, one observes that the elements of G are either 7-elements or 3-elements. If $x \in G$ is a 7-element, then $N_G(\langle x\rangle)$ is a Frobenius group of order 21 and hence x is semi-rational in G. If x is a 3-element, then x belongs to a Sylow 3-subgroup P of G. One checks easily that P is semi-rational. Hence G is semi-rational. We also observe that $\exp(P) = 9$.

We give, finally, examples of semi-rational groups of even order.

Example 3. Let H be a Hall $\{2, 3\}$-subgroup of $\mathrm{SL}(2, 7)$. Then $|H| = 48$ and $H' \simeq \mathrm{SL}(2, 3)$. Let $G = V \rtimes H$ be the semidirect product of H with the natural module $V = V(2, 7)$. Then G is semi-rational, but not inverse semi-rational.

Moreover, $G' = V \rtimes H'$ is inverse semi-rational.

Remark 14. A Sylow 2-subgroup of the symmetric group S_{2^n} of degree 2^n is a rational group and its derived length and exponent increase as n increases. Likewise, a Sylow 3-subgroup of the symmetric group S_{3^n} of degree 3^n is inverse semi-rational, and it has derived length and exponent that increase with n. Hence there is no upper bound for either the derived length or the exponent of a solvable semi-rational group.

We finish by mentioning some open problems.

Problem 1. Let G be a solvable semi-rational group and $\mathbb{K}$ the field generated by the values of all irreducible characters of G. Is there an upper bound for the degree $[\mathbb{K} : \mathbb{Q}]$?

Problem 2. Let G be a solvable group and k a positive integer. We say that element $x \in G$ is *k-semi-rational in G* if $|B_G(x)|$ has at most k orbits on the set of generators of $\langle x\rangle$. (If $k = 1$ then x is rational and if $k = 2$ then x is semi-rational.) If every element is k-semi-rational in G, then is $|\pi(G)|$ bounded in terms of k?

Acknowledgments. The second author thanks the Department of Mathematics at the Technion for the warm hospitality. The authors are grateful to the referee for pointing out Remark 14.

References

[1] W. Feit and G. M. Seitz. On finite rational groups and related topics. *Illinois J. Math.* **33** (1989), 103–131.
[2] P. Fitzpatrick. Order conjugacy in finite groups. *Proc. Roy. Irish Acad. Sect. A* **85** (1985), 53–58.
[3] R. Gow. Groups whose characters are rational-valued. *J. Algebra* **40** (1976), 280–299.
[4] G. Higman. Finite groups in which every element has prime power order. *J. London Math. Soc.* **32** (1957), 335–342.
[5] M. Herzog and J. Schonheim. On groups of odd order with exactly two non-central conjugacy classes of each size. *Arch. Math.* (*Basel*) **86** (2006), 7–10.
[6] B. Huppert. *Endliche Gruppen*, vol. 1 (Springer-Verlag, 1967).
[7] R. Knörr, W. Lempken and B. Thielke. The S3-conjecture for solvable groups. *Israel J. Math.* **91** (1995), 61–76.
[8] C. H. Li. Finite groups in which every pair of elements of the same order is either conjugate or inverse-conjugate. *Comm. Algebra* **22** (1994), 2807–2816.
[9] D. Passman. *Permutation groups* (W. A. Benjamin, 1968).
[10] E. Farias e Soares. Big primes and character values for solvable groups. *J. Algebra* **100** (1986), 305–324.
[11] J. P. Zhang. Finite groups with many conjugate elements. *J. Algebra* **170** (1994), 608–624.

Received 18 May, 2009; revised 23 September, 2009

David Chillag, Department of Mathematics, Technion, Israel Institute of Technology, Haifa 32000, Israel
E-mail: chillag@techunix.technion.ac.il

Silvio Dolfi, Dipartimento di Matematica U. Dini, Università degli Studi di Firenze, Viale Morgagni 67/a, 50134 Firenze, Italy