TALK IN BIELEFELD

IN HONOUR OF BERND FISCHER

A NEW SOLVABILITY CRITERION FOR FINITE GROUPS

MARCH 14, 2012

Marcel Herzog

School of Mathematical Sciences
Tel-Aviv University,
Tel-Aviv, Israel

This is a joint paper with

Silvio Dolfi
Bob Guralnick
and
Cheryl Praeger

to appear in the

Journal of the London Mathematical Society.

See: http://arxiv.org/abs/1105.0475 .

I. **Introduction.**

John G. Thompson's famous

'N-group paper'

of 1968 included the following important solvability criterion for finite groups:

Thompson's theorem. *A finite group is solvable if and only if every pair of its elements generates a solvable group.*

In 1995, Paul Flavell published a relatively simple proof of Thompson's result.

We proved that solvability of a finite group is guaranteed by a seemingly weaker condition than the solvability of all its 2-generator subgroups.

Theorem A. *Let G be a finite group. The following statements are equivalent:*

(1) *G is solvable;*

(2) *For all $x, y \in G$, there exists an element $g \in G$ for which $\langle x, y^g \rangle$ is solvable; and*

(3) *For all $x, y \in G$ of prime power order, there exists an element $g \in G$ for which $\langle x, y^g \rangle$ is solvable.*

Theorem A can be rephrased as the following essentially equivalent result.

Theorem A'. *Let G be a finite group such that, for all distinct conjugacy classes C and D of G consisting of elements of prime power order, there exist $x \in C$ and $y \in D$ for which $\langle x, y \rangle$ is solvable. Then G is solvable.*

Our second main result, which is the key tool for proving Theorem A, deals with the nonsolvability of certain 2-generator subgroups of finite nonabelian simple groups. Using the classification of finite simple groups, we proved the following theorem.

Theorem B. *Let G be a finite nonabelian simple group. Then there exist distinct prime divisors p, q of $|G|$ such that, for all $x, y \in G$ with $|x| = p$, $|y| = q$, the subgroup $\langle x, y \rangle$ is nonsolvable.*

Theorem A can also be used to give the following characterization of finite nilpotent groups. Our proof depends upon the finite simple groups classification, since Theorem A does. It would be interesting to see if this result could be proved without the classification of finite simple groups.

Corollary C. *Let G be a finite group. Then G is nilpotent if and only if for every pair of distinct primes p and q and for every pair of elements $x, y \in G$ with x a p-element and y a q-element, x and y^g commute for some $g \in G$.*

We can restate Theorem A in an analogous manner.

Corollary D. *Let G be a finite group. Then G is solvable if and only if for every pair of distinct primes p and q and for every pair of elements $x, y \in G$ with x a p-element and y a q-element, $\langle x, y^g \rangle$ is a $\{p, q\}$-group for some $g \in G$.*

II. **Other generalisations of Thompson's theorem.**

Several other "Thompson-like" results have appeared in the literature recently. We mention here five such theorems. In three of them solvability of all 2-generator subgroups is replaced by a weaker condition, restricting the required set of solvable 2-generator subgroups.

In 2000, Wilson and Guralnick obtained a solvability criterion by **restricting the proportion of 2-generator subgroups** required to be solvable.

Theorem 2.1. *A finite group is solvable if and only if more than* $\frac{11}{30}$ *of the pairs of elements of* G *generate a solvable subgroup.*

In addition, they proved similar results showing that the properties of nilpotency and of "having odd order" are also guaranteed if a sufficient proportion of element pairs generate subgroups with these properties.

Theorem 2.2. *A finite group is nilpotent (of odd order) if and only if more than* $\frac{1}{2}$ *(*$\frac{11}{30}$*) of the pairs of elements of* G *generate a nilpotent (of odd order) subgroup.*

In contrast to this, in a paper published in 2009, Gordeev, Grunewald, Kunyavskiĭ and Plotkin proved a solvability criterion which involved **2-generation within each conjugacy class**. This result was also proved independently by Simon Guest.

Theorem 2.3. *A finite group G is solvable if and only if, for each conjugacy class C of G, each pair of elements of C generates a solvable subgroup.*

A stronger result of this type follows easily from a result of Guest, while a slightly weaker version of it was obtained recently by Kaplan and Levy. Their criterion involves only a **limited 2-generation within the conjugacy classes of elements of odd prime-power order**.

Theorem 2.4. *A finite group G is solvable if and only if, for all $x, y \in G$ with x a p-element for each prime $p > 3$ dividing $|G|$ and y a 2-element, the group $\langle x, x^y \rangle$ is solvable.*

The requirement in our theorem, while ranging over all conjugacy classes, requires only the **existence** of a solvable 2-generator subgroup with one generator from each of two classes.

We know of no similar criteria in this respect.

The fifth result we wish to draw your attention to is in a 2006 paper of Guralnick, Kunyavskiĭ, Plotkin and Shalev. They proved that membership of the solvable radical of a finite group is characterised by solvability of certain 2-generator subgroups. (The **solvable radical** $R(G)$ of a finite group G is the largest solvable normal subgroup of G.)
They proved the following theorem.

Theorem 2.5. *For a finite group G, the solvable radical $R(G)$ coincides with the set of all elements $x \in G$ with the following property:*

for any $y \in G$, the subgroup $\langle x, y \rangle$ is solvable.

In view of the previous results, it might seem reasonable to consider the following conjecture.

Conjecture. *For a finite group G, the solvable radical $R(G)$ coincides with the set of all elements $x \in G$ with the following property:*

for any $y \in G$, there exists $g \in G$ such that

the subgroup $\langle x, y^g \rangle$ is solvable.

However, this conjecture is **false**.

For example, the group A_5 contains solvable subgroups of order 6 and 10, and it consists of the unit elements, one class of elements of order 2, one class of elements of order 3 and two classes of elements of order 5. So if $x \in A_5$ is of order 2, then it generates a solvable subgroup with some conjugate of each element of A_5, while certainly the involution x does not belong to the solvable radical of A_5. The same holds for elements of order 3 in $PSL(2,7)$ and Simon Guest and Cheryl Praeger have constructed such counterexamples for elements x of an arbitrary prime order.

The aim of the rest of this lecture is to present a rough sketch of the proof of Theorem B, including some useful lemmas, and to apply it for the proof of Theorem A.

III. **On the proof of Theorem B.**

First we remind you the statement of Theorem B.

Theorem B. *Let G be a finite nonabelian* **simple group**. *Then there exist distinct prime divisors p, q of $|G|$ such that, for all $x, y \in G$ with $|x| = p$, $|y| = q$, the subgroup $\langle x, y \rangle$ is nonsolvable.*

By the classification of the finite simple groups, we need to consider the following four types of simple groups:

(a) Alternating groups A_n for $n \geq 5$.

(b) The 26 sporadic simple groups.

(c) Classical simple groups of Lie type.

(d) Exceptional simple groups of Lie type.

We consider first the proof of Theorem B for the alternating and sporadic simple groups. We need the following useful lemma.

Lemma 3.1. *Let H be a finite group and let p, q be distinct prime divisors of $|H|$. Assume that the following statements hold.*

(1) *The Sylow q-subgroup of H is cyclic and the Sylow p-subgroup of H has order p^s.*

(2) *p does not divide $q - 1$.*

(3) *q does not divide $p^m - 1$ for $1 \leq m \leq s$ (certainly holds if $q > p^s$); and*

(4) *H contains no elements of order pq.*

Then H contains no subgroup of order $p^a q^b$ with $a, b > 0$.

In particular, H is nonsolvable.

Proof. Suppose, to the contrary, that H contains a subgroup B of order $p^a q^b$ with $a, b > 0$. Our aim is to reach a contradiction.

Let N be a minimal normal subgroup of B. Since B is solvable, N is elementary abelian.

If N is a q-group, then by (1) $|N| = q$ and B contains a subgroup M of order pq. Hence, either M is nonabelian, in which case p divides $q - 1$, in contradiction to (2), or M is abelian, hence cyclic of order pq, in contradiction to (4). Thus N is not a q-group.

If N is a p-group, then by (1) $|N| = p^i \leq p^s$ and hence B contains a subgroup $M > N$ of order qp^i.

Since by (4) H contains no elements of order pq, an element of order q in M acts fixed point freely on N, which implies that q divides $p^i - 1$, in contradiction to (3).

Thus B does not exist, as required. $\square$

First we sketch a proof of

Proposition 3.2. *Theorem B holds for the alternating simple groups.*

Proof. Note that if m is a positive integer and $\pi(m)$ denotes the number of primes at most m, then the following is known:

$$\pi(2m) - \pi(m) > m/(3 \ln 2m) \quad \text{for} \quad m > 1.$$

Now,

$$m/(3 \ln 2m) \geq 2 \quad \text{for} \quad m \geq 9 \ .$$

so it follows that

$$\pi(n) - \pi(n/2) \geq 2 \quad \text{for} \quad n \geq 18 \ .$$

This implies, in particular, that there exist primes p, q such that

$$n/2 \leq p < q \leq n \quad \text{for} \quad n \geq 18 \ .$$

It can be shown, by checking small values of n, that the above statement holds for all $n \geq 5$. This is only true because we allow $p = n/2$. For examle, if $n = 10$, we have

$$\frac{n}{2} = 5 = p < q = 7 < n = 10$$

and no other choice of the primes p, q is possible.

So let $n \geq 5$ and choose primes p and q as indicated above. Then $p + q > n$ and no element of A_n contains either disjoint cycles of both lengths p and q or a cycle of length pq. Thus A_n contains no elements of order pq.

Moreover, as $q > \frac{n}{2}$, the Sylow q-subgroup of A_n is cyclic of order q and it follows from

$$q - 1 > p \geq q/2$$

that p does not divide $q - 1$ and q does not divide $p^2 - 1$ (if $n = 10$, then $p = 5$ and p^2 divides $|A_{10}|$).

Let $x, y \in A_n$, with $|x| = p$ and $|y| = q$. Then $H = \langle x, y \rangle$ satisfies the assumptions of Lemma 3.1, and hence $\langle x, y \rangle$ is nonsolvable. Thus A_n satisfies Theorem B with respect to these primes. $\square$

Next we sketch a proof of

Proposition 3.3. *Theorem B holds for the sporadic simple groups.*

Proof. We shall describe the treatment of the sporadic simple group M_{12}, where

$$|M_{12}| = 95,040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11 \ .$$

The treatment of all the other sporadic simple groups is similar.

We choose $p = 3$ and $q = 11$. The choice $p = 5$ and $q = 11$ is inappropriate, since 5 divides $11 - 1$.

Let $x, y \in M_{12}$, with $|x| = p = 3$ and $|y| = q = 11$ and let $H = \langle x, y \rangle$. We shall show now that M_{12}, and hence also H, fulfills the conditions of Lemma 3.1.

(1) The Sylow 11-subgroup of M_{12} is of order 11, hence it is cyclic. The Sylow 3 subgroup of M_{12} is of order 3^3.

(2) 3 does not divide $11 - 1$.

(3) 11 does not divide $3^m - 1$ for $1 \leq m \leq 3$.

(4) By the ATLAS, M_{12} contains no element of order $3 \cdot 11 = 33$.

Hence, by Lemma 3.1, $H = \langle x, y \rangle$ is nonsolvable, as required. $\square$

We now consider the simple groups of Lie type. Here the situation is much more complicated. We shall describe here only one simple case. In order to do so, we need the following lemma.

Lemma 3.4. *Let H be a finite group and let p, q be distinct primes dividing $|H|$. Suppose that the Sylow p- and q-subgroups of H are both cyclic, and H contains no subgroup of order pq. Then H is nonsolvable.*

Proof. Suppose, to the contrary, that H is solvable and let M be a Hall $\{p, q\}$-subgroup of H. Let, now, N be a minimal normal subgroup of M. Then, since the Sylow p- and q-subgroups of H are both cyclic, N is of prime order, say p, and M contains a subgroup of order pq, a contradiction. Hence H is nonsolvable, as required. $\square$

We are now ready to prove the following proposition.

Proposition 3.5. *Theorem B holds for the simple groups $PSL(2, 2^a)$, with $2^a \geq 4$.*

Proof. We have

$$|PSL(2, 2^a)| = (2^a - 1)2^a(2^a + 1) \ .$$

Let p be a prime dividing $2^a - 1$ and let q be a prime dividing $2^a + 1$. Clearly both p and q are odd primes.

Since $PSL(2, 2^a)$ contains cyclic subgroups of orders $2^a - 1$ and $2^a + 1$, the Sylow p-subgroup and the Sylow q-subgroup of $PSL(2, 2^a)$ are cyclic.

Let x be an element of $PSL(2, 2^a)$ of order p and let y be an element of $PSL(2, 2^a)$ of order q.

Denote $H = \langle x, y \rangle$. Since the Sylow p-subgroup and the Sylow q-subgroup of $PSL(2, 2^a)$ are cyclic, also the Sylow p-subgroup and the Sylow q-subgroup of H are cyclic. Moreover, for each element u of $PSL(2, 2^a)$ of order p we have

$$|N_{PSL(2,2^a)}(\langle u \rangle)| = 2(2^a - 1)$$

and for each element v of $PSL(2, 2^a)$ of order q we have

$$|N_{PSL(2,2^a)}(\langle v \rangle)| = 2(2^a + 1) \ .$$

In particular, pq divides neither $|N_{PSL(2,2^a)}(\langle u \rangle)|$ nor $|N_{PSL(2,2^a)}(\langle v \rangle)|$.

Hence H contains no subgroups of order pq, since any subgroup of $PSL(2, 2^a)$ of order pq would be contained in one of such normalizers, which is impossible.

Thus H satisfies the conditions of Lemma 3.4 and, consequently, $H = \langle x, y \rangle$ is nonsolvable, as required. $\square$

IV. **The proof of Theorem A.**

This is the final section of this talk.

Our aim here is twofold:

(i) to show how Theorem B leads us to a proof of Theorem A;

(ii) to show that Theorem A is almost best possible.

We start with the statements of the theorems, beginning with Theorem B.

Theorem B. *Let G be a finite nonabelian* **simple group**. *Then there exist distinct* **prime divisors** *p, q of $|G|$ such that, for all $x, y \in G$ with $|x| = p$ and $|y| = q$, the subgroup $\langle x, y \rangle$ is nonsolvable.*

Next we state Theorem A, which we intend to prove.

Theorem A. *Let G be a finite group.*

The following statements are equivalent:

(1) *G is solvable;*

(2) *For all $x, y \in G$, there exists an element $g \in G$ for which $\langle x, y^g \rangle$ is solvable; and*

(3) *For all $x, y \in G$* **of prime power order**, *there exists an element $g \in G$ for which $\langle x, y^g \rangle$ is solvable.*

Proof of Theorem A. The implications (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are obvious. We need only to prove that (3) $\Rightarrow$ (1).

So let G be a finite group such that, if $x, y \in G$ are of prime power order, then $\langle x, y^g \rangle$ is solvable for some $g \in G$. In other words, let G satisfy hypothesis (3). We need to prove that G is solvable.

Suppose that this is **not the case**, and let the non-solvable group G be a minimal counterexample.

Our aim is to reach a contradiction.

By Theorem B, if G is simple, then hypothesis (3) couldn't hold. Therefore G is non-simple.

Let N be a minimal normal subgroup of G.
Since G is non-simple, N is a proper subgroup of G.

Note that if $xN \in G/N$ is of prime power order, then we may replace x by a power of itself and assume that also x is of prime power order.

Thus, if $xN, yN \in G/N$ are of prime power order, we may assume that x, y are elements of G of prime power order, and by our assumptions, $\langle x, y^g \rangle$ is solvable for some $g \in G$. Hence also $\langle xN, (yN)^{gN} \rangle$ is solvable and G/N satisfies hypothesis (3).

Thus it follows, by the minimality of G, that G/N is solvable.

Since G is non-solvable and G/N is solvable, it follows that N is a nonsolvable minimal normal subgroup of G. Therefore

$$N = L_1 \times \ldots \times L_t \cong L^t$$

for some nonabelian simple group L and $t \geq 1$.

By Theorem B there exist distinct primes p, q dividing $|L|$ such that $\langle a, b \rangle$ is nonsolvable for all $a, b \in L$ of order p and q, respectively.

Since $L_i \cong L$ for $1 \leq i \leq t$, $\langle a, b \rangle$ is nonsolvable for all $a, b \in L_i$ of order p and q, respectively.

Let now x_i, y_i be elements of L_i of order p and q, respectively, where $N = L_1 \times \ldots \times L_t \cong L^t$. Moreover, let

$$x = (x_1, \ldots, x_t) \in N \quad \text{and} \quad y = (y_1, \ldots, y_t) \in N.$$

If $g \in G$, then $\langle x, y^g \rangle$ is a subgroup of N.

Now y_1^g is an element of L_i for some i and $|y_1^g| = q$. Thus the projection of $\langle x, y^g \rangle$ to L_i contains $\langle x_i, y_1^g \rangle$, where $|x_i| = p$ and $|y_1^g| = q$. Since, by our choice of p and q, $\langle x_i, y_1^g \rangle$ is non-solvable, it follows that the projection of $\langle x, y^g \rangle$ to L_i is non-solvable. Hence also $\langle x, y^g \rangle$ is non-solvable.

As this holds for each $g \in G$, we obtained a contradiction to hypothesis (3), which requires $\langle x, y^g \rangle$ to be solvable for some $g \in G$.

The proof of Theorem A is complete. $\square$

Theorem A is very nice, but a question arises: Is Theorem A best possible?

Recall Theorem B:

Theorem B. *Let G be a finite nonabelian simple group. Then there exist distinct* **prime divisors** *p, q of $|G|$ such that, for all $x, y \in G$ with $|x| = p$ and $|y| = q$, the subgroup $\langle x, y \rangle$ is nonsolvable.*

In view of Theorem B, it is tempting to consider the following conjecture:

Conjecture A. *Let G be a finite group.*

The following statements are equivalent:

(1) *G is solvable;*

(2) *For all $x, y \in G$* **of prime order**,
there exists an element $g \in G$ for which $\langle x, y^g \rangle$ is solvable.

Unlike Theorem A, which deals with $x, y \in G$ **of prime power order**, Conjecture A requires only that given elements x, y of G **of prime order**, there exists $g \in G$ for which $\langle x, y^g \rangle$ is solvable.

Recall that in our proof of Theorem A we needed the stronger assumption, because if xN is an element of G/N of **prime order**, we know only that x may be replaced by an element of G of **prime power order**.

Is our stronger assumption really necessary?

The answer is: YES.

The weaker inductive assumption, dealing only with elements of prime order, is not sufficient!

This fact was noticed by Enrico Jabara.

Jabara showed that there exists a non-split extension

$$G_1 = (C_3)^4 * SL(2,5)$$

of order 9720, with the Fitting subgroup

$$F(G) = (C_3)^4 \times C_2,$$

and the orders of elements in $G - F(G)$ are

$$\{4, 5, 9, 10, 12.18\}.$$

Hence, if $x, y \in G_1$ are of distinct prime orders, then at least one of them lies in $F(G)$ and $\langle x, y \rangle$ is solvable. If, on the other hand, $|x| = |y| = 5$, then there exists z, a conjugate of y, such that $\langle x, z \rangle$ is solvable.

But clearly G_1 is non-solvable!

Moreover, Jabara claims that there exists a non-split extension

$$G_2 = ((C_3)^4 \times (C_5)^3) * SL(2,5)$$

with

$$F(G) = (C_3)^4 \times (C_5)^3 \times C_2,$$

and **all elements** of G_2 of prime order lie in $F(G)$.

Thus Theorem A is close to being best possible.

My talk is now complete.

THANK YOU FOR YOUR ATTENTION.