Luca Sabatini (University of Warwick)

*Arithmetical properties of subgroup products*

Seminars on Groups and Graphs (2025)

Let $G$ be a finite group, $x \in G$, and $H \leqslant G$.
It is easy to see that

- $x^{|G|} = 1$;
- if $H \lhd G$, then $x^{|G:H|} \in H$;

Let $G$ be a finite group, $x \in G$, and $H \leqslant G$.
It is easy to see that

- $x^{|G|} = 1$;
- if $H \lhd G$, then $x^{|G:H|} \in H$;
- if $G = \mathrm{Sym}(3)$, $x = (1\,2)$ and $H = \langle (1\,3) \rangle$, then

$$x^{|G:H|} = x \notin H.$$

Let $G$ be a finite group, $x \in G$, and $H \leqslant G$.
It is easy to see that

- $x^{|G|} = 1$;
- if $H \lhd G$, then $x^{|G:H|} \in H$;
- if $G = \mathrm{Sym}(3)$, $x = (1\,2)$ and $H = \langle (1\,3) \rangle$, then

$$x^{|G:H|} = x \notin H.$$

Three questions arise:

- (i) Understand better when $x^{|G:H|} \in H$ holds;

Let $G$ be a finite group, $x \in G$, and $H \leqslant G$.
It is easy to see that

- $x^{|G|} = 1$;
- if $H \lhd G$, then $x^{|G:H|} \in H$;
- if $G = \mathrm{Sym}(3)$, $x = (1\,2)$ and $H = \langle (1\,3) \rangle$, then

$$x^{|G:H|} = x \notin H.$$

Three questions arise:

- (i) Understand better when $x^{|G:H|} \in H$ holds;
- (ii) Describe the set $\{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G\}$;

Let $G$ be a finite group, $x \in G$, and $H \leqslant G$.
It is easy to see that

- $x^{|G|} = 1$;
- if $H \lhd G$, then $x^{|G:H|} \in H$;
- if $G = \mathrm{Sym}(3)$, $x = (1\,2)$ and $H = \langle (1\,3) \rangle$, then

$$x^{|G:H|} = x \notin H.$$

Three questions arise:

- (i) Understand better when $x^{|G:H|} \in H$ holds;
- (ii) Describe the set $\{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G\}$;
- (iii) What are the subgroups $H$ where $x^{|G:H|} \in H$ for all $x \in G$?

We start dealing with Question (i).

If $H \lhd M \lhd G$, then
$$x^{|G:H|} = (x^{|G:M|})^{|M:H|},$$
and for some $m \in M$,
$$x^{|G:H|} = m^{|M:H|} \in H.$$

We start dealing with Question (i).

If $H \lhd M \lhd G$, then

$$x^{|G:H|} = (x^{|G:M|})^{|M:H|},$$

and for some $m \in M$,

$$x^{|G:H|} = m^{|M:H|} \in H.$$

As a consequence, subnormal subgroups satisfy (iii).

However, this approach does not go far. In fact, even if both

$$x^{|G:H|} \in H \quad \text{and} \quad y^{|G:H|} \in H$$

hold for some fixed $H$, it might happen that $(xy)^{|G:H|} \notin H$.
In contrast, we will see that the set in (ii) is closed under multiplication!

A wider perspective is needed.

## Definition

For $x \in G$ and $H \leqslant G$, the **relative order** of $x$ with respect to $H$ is defined as

$$o_H(x) \ := \ \min\{n \geq 1 : x^n \in H\}.$$

Moreover, we write $o(x) = o_1(x)$ for the genuine order.

A wider perspective is needed.

### Definition

For $x \in G$ and $H \leqslant G$, the **relative order** of $x$ with respect to $H$ is defined as

$$o_H(x) \; := \; \min\{n \geq 1 : x^n \in H\}.$$

Moreover, we write $o(x) = o_1(x)$ for the genuine order.

**Remark:** Using the subgroup structure of $H$, it is easy to see that

$$x^n \in H \quad \text{if and only if} \quad o_H(x) \text{ divides } n.$$

## Lemma

$$o_H(x) = \frac{o(x)}{|H \cap \langle x \rangle|}.$$

## Proof.

Note that $o_H(x) = o_{H\cap\langle x\rangle}(x)$ and work in a cyclic group. □

**Lemma**

$$o_H(x) = \frac{o(x)}{|H \cap \langle x \rangle|}.$$

**Proof.**

Note that $o_H(x) = o_{H\cap\langle x\rangle}(x)$ and work in a cyclic group. □

**Corollary**

*$x^{|G:H|} \in H$ if and only if $|H\langle x\rangle|$ divides $|G|$.*

**Proof.**

$o(x) = |\langle x\rangle|$, so $o_H(x) = |H\langle x\rangle : H|$. Now use the remark. □

Let $H, K \leqslant G$. It is well known that $HK$ is a subgroup if and only if $HK = KH$. Moreover, $H$ is called **permutable** if this holds for all $K$.

In 1937, Ore proved that permutable subgroups are subnormal.

Let $H, K \leqslant G$. It is well known that $HK$ is a subgroup if and only if $HK = KH$. Moreover, $H$ is called **permutable** if this holds for all $K$.

In 1937, Ore proved that permutable subgroups are subnormal.

We observe the following:

**Lemma**

*If $HC = CH$ for every cyclic $C \leqslant G$ then $H$ is permutable.*

**Proof.**

Let $K \leqslant G$. Then $K = C_1 \cdots C_n$ for some cyclic subgroups $C_1, \ldots, C_n$. □

If $HK$ is a subgroup, then certainly $|HK|$ divides $|G|$.

The latter is a much weaker condition: $D_8$ is generated by two subgroups $H$ and $K$ of order 2, so $HK$ has order 4, but is **not** a subgroup.

If $HK$ is a subgroup, then certainly $|HK|$ divides $|G|$.

The latter is a much weaker condition: $D_8$ is generated by two subgroups $H$ and $K$ of order 2, so $HK$ has order 4, but is **not** a subgroup.

In general,

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

and there is no reason for this to be a divisor of $|G|$.

**Remark:** $|HK|/|H|$ is the number of right cosets of $H$ intersected by $K$.

As it can be expected, Sylow subgroups play a key role.

## Lemma

Let $H \leqslant G$. If $|HP|$ divides $|G|$ for every Sylow $P \leqslant G$, then $|HK|$ divides $|G|$ for every $K \leqslant G$.

## Proof.

Let $K \leqslant G$. We have to show that $|HK : K|$ divides $|G : K|$. Let $p^\alpha$ divide $|H : H \cap K|$. Let $P_0 \in \mathrm{Syl}_p(K)$ and $P \in \mathrm{Syl}_p(G)$ such that $P \cap K = P_0$. Of course, $p^\alpha$ divides $|H : H \cap P_0|$. By hypothesis $|H : H \cap P| = |HP : P|$ divides $|G : P|$, and so is not divisible by $p$. Therefore, $p^\alpha$ divides $|H \cap P : H \cap P_0|$. This is equal to $|(H \cap P)P_0 : P_0|$ and divides $|P : P_0|$. So $p^\alpha$ divides $|P : P_0|$, and in particular divides $|G : P_0|$. Since $p \nmid |K : P_0|$, $p^\alpha$ divides $|G : K|$ as desired. □

The following is a crucial observation.

## Lemma

Let $H \leqslant G$ and let $P \in \mathrm{Syl}_p(G)$. Then

$$|HP| \text{ divides } |G| \text{ if and only if } H \cap P \text{ is a } p\text{-Sylow of } H.$$

## Proof.

$H \cap P \in \mathrm{Syl}_p(H)$ if and only if $|H : H \cap P| = |HP : P|$ is not divisible by $p$. Since $|H : H \cap P|$ is a divisor of $|G|$, the last condition is equivalent to $|HP : P|$ dividing $|G : P|$, i.e. $|HP|$ dividing $|G|$. □

The point is that the subgroups $H$ with the property that

$$P \text{ is a Sylow of } G \quad \Longrightarrow \quad H \cap P \text{ is a Sylow of } H$$

have been studied in depth. In particular, Kegel and Wielandt independently conjectured that this should be equivalent to subnormality.

The point is that the subgroups $H$ with the property that

$$P \text{ is a Sylow of } G \quad \Longrightarrow \quad H \cap P \text{ is a Sylow of } H$$

have been studied in depth. In particular, Kegel and Wielandt independently conjectured that this should be equivalent to subnormality.

In 1991, Kleidman proved that this is actually true.

**Theorem (Kleidman)**

$H \lhd \lhd G$ if and only if $H \cap P$ is a Sylow of $H$ for all Sylow $P$ of $G$.

The point is that the subgroups $H$ with the property that

$$P \text{ is a Sylow of } G \quad \Longrightarrow \quad H \cap P \text{ is a Sylow of } H$$

have been studied in depth. In particular, Kegel and Wielandt independently conjectured that this should be equivalent to subnormality.

In 1991, Kleidman proved that this is actually true.

**Theorem (Kleidman)**

$H \lhd \lhd G$ if and only if $H \cap P$ is a Sylow of $H$ for all Sylow $P$ of $G$.

From the discussion above, we have

**Theorem (Kleidman's theorem revisited)**

$H \lhd \lhd G$ if and only if $|HK|$ divides $|G|$ for all $K \leqslant G$.

The following lemma proves one direction of the revisited conjecture:

**Lemma**

Let $H \lhd M \leqslant G$, and $K \leqslant G$. Then $|HK|$ divide $|MK|$.

**Proof.**

With some computations we have

$$\frac{|MK|}{|HK|} = \frac{|M|}{|H(M \cap K)|}.$$

The proof follows because $H(M \cap K)$ is a subgroup of $M$. □

The following lemma proves one direction of the revisited conjecture:

**Lemma**

Let $H \lhd M \leqslant G$, and $K \leqslant G$. Then $|HK|$ divide $|MK|$.

**Proof.**

With some computations we have

$$\frac{|MK|}{|HK|} = \frac{|M|}{|H(M \cap K)|}.$$

The proof follows because $H(M \cap K)$ is a subgroup of $M$. □

To prove the easy direction, let $H \lhd \lhd G$ and $K \leqslant G$. Then start with $M = G$ and iterate the lemma on the subnormal series.

Now we deal with the opposite (hard) direction.

We first observe that a very short argument exists when $H$ is nilpotent.

## Theorem

Let $H \leqslant G$ be nilpotent and let $|HK|$ divide $|G|$ for all $K \leqslant G$.
Then $H \lhd \lhd G$.

## Proof.

Suppose that $H$ is not subnormal, so that in particular $H \nsubseteq F(G)$.
Then there exists a $p$-element $x \in H \setminus O_p(G)$,
i.e. there exists $P \in \mathrm{Syl}_p(G)$ such that $x \notin P$.
By cardinality reasons, $|\langle x \rangle P|$ cannot divide $|G|$.
Since $H$ is nilpotent we have $\langle x \rangle \lhd \lhd H$.
From the discussion above $|HP|$ is a multiple of $|\langle x \rangle P|$.
This implies that $|HP|$ cannot divide $|G|$, which gives a contradiction. □

The problem with the general case is that $|HP|$ is not always a multiple of $|\langle x \rangle P|$. In fact it is possible that $|\langle x \rangle P|$ does not divide $|G|$ while $|HP|$ does.

The problem with the general case is that $|HP|$ is not always a multiple of $|\langle x\rangle P|$. In fact it is possible that $|\langle x\rangle P|$ does not divide $|G|$ while $|HP|$ does.

The proof of Kleidman is much more ingenious. Here we give a sketch. With some work, he reduces to the situation where both $G$ and $H$ are simple. Now, if $x \in G$ is a $p$-element and $P \in \mathrm{Syl}_p(G)$, he defines the **fixed point ratio**

$$\Theta_G(x) := \frac{|x^G \cap P|}{|x^G|}.$$

The problem with the general case is that $|HP|$ is not always a multiple of $|\langle x\rangle P|$. In fact it is possible that $|\langle x\rangle P|$ does not divide $|G|$ while $|HP|$ does.

The proof of Kleidman is much more ingenious. Here we give a sketch. With some work, he reduces to the situation where both $G$ and $H$ are simple. Now, if $x \in G$ is a $p$-element and $P \in \mathrm{Syl}_p(G)$, he defines the **fixed point ratio**

$$\Theta_G(x) := \frac{|x^G \cap P|}{|x^G|}.$$

For $h \in H$, the condition $H \cap P \in \mathrm{Syl}_p(H)$ implies that $\Theta_G(h) = \Theta_H(h)$. On the other hand, he proves using CFSG that $\Theta_G(h) < \Theta_H(h)$ except in a few cases where $H$ is a “large” subgroup. These cases are handled separately.

We come to Question (ii).

### Definition

$$S(G) := \{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G\}.$$

We come to Question (ii).

## Definition

$$S(G) := \{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G\}.$$

## Theorem

*$S(G) = F(G)$.*

## Proof.

From the discussion above we have

$$S(G) = \{x \in G : |H\langle x\rangle| \text{ divides } |G| \text{ for all } H \leqslant G\}.$$

Since $G$ is finite, $F(G)$ can be described as the set of $x \in G$ such that $\langle x\rangle \lhd \lhd G$. So, if $x \in F(G)$, then $x \in S(G)$ by the easy direction of the K-W conjecture. Viceversa, let $x \in S(G)$. Being $\langle x\rangle$ nilpotent, we can conclude with an elementary argument that $\langle x\rangle \lhd \lhd G$, and so that $x \in F(G)$. □

We dedicate just one slide to infinite groups. In fact, $S(G)$ can still be defined as

$$S(G) := \{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G \textit{ of finite index}\}.$$

Here we have to distinguish between

- $F(G) = \{x \in G : \langle x \rangle^G \text{ is nilpotent}\}$;
- $B(G) = \{x \in G : \langle x \rangle \text{ is subnormal}\}$, the **Baer radical**.

The argument above shows that $F(G) \subseteq B(G) \subseteq S(G)$.

We dedicate just one slide to infinite groups. In fact, $S(G)$ can still be defined as

$$S(G) := \{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G \textit{ of finite index}\}.$$

Here we have to distinguish between

- $F(G) = \{x \in G : \langle x \rangle^G \text{ is nilpotent}\}$;
- $B(G) = \{x \in G : \langle x \rangle \text{ is subnormal}\}$, the **Baer radical**.

The argument above shows that $F(G) \subseteq B(G) \subseteq S(G)$.

Some attention is needed with subgroups of infinite index:

**Example:** Let $G$ be a *just-infinite* $p$-group.
Then $G = S(G)$, but $B(G) = 1$ (Wilson '71).

We dedicate just one slide to infinite groups. In fact, $S(G)$ can still be defined as

$$S(G) := \{x \in G : x^{|G:H|} \in H \text{ for all } H \leqslant G \textit{ of finite index}\}.$$

Here we have to distinguish between

- $F(G) = \{x \in G : \langle x \rangle^G \text{ is nilpotent}\}$;
- $B(G) = \{x \in G : \langle x \rangle \text{ is subnormal}\}$, the **Baer radical**.

The argument above shows that $F(G) \subseteq B(G) \subseteq S(G)$.

Some attention is needed with subgroups of infinite index:

**Example:** Let $G$ be a *just-infinite* $p$-group.
Then $G = S(G)$, but $B(G) = 1$ (Wilson '71).
Moreover, let $H$ be a nilpotent subgroup. Then $H$ is not subnormal in $G$, but $|HK : K|$ divides $|G : K|$ for all $K \leqslant G$ of finite index.

We go back to the finite world, to address Question (iii).

## Definition

$H \leqslant G$ is **exponential** if $x^{|G:H|} \in H$ for all $x \in G$.

Equivalently,

$$H \leqslant_{exp} G \text{ if and only if } |HC| \text{ divides } |G| \text{ for all } \textit{cyclic } C \leqslant G.$$

Some facts ($\exp(G)$ denotes the **exponent** of $G$):

- The subnormal subgroups are exponential;
- $H$ is exponential if $|G : H|$ is a multiple of $\exp(G)$;

Some facts ($\exp(G)$ denotes the **exponent** of $G$):

- The subnormal subgroups are exponential;
- $H$ is exponential if $|G : H|$ is a multiple of $\exp(G)$;
- being exponential is a transitive relation;

Some facts ($\exp(G)$ denotes the **exponent** of $G$):

- The subnormal subgroups are exponential;
- $H$ is exponential if $|G : H|$ is a multiple of $\exp(G)$;
- being exponential is a transitive relation;
- the intersection of exponential subgroups is exponential.

Some facts ($\exp(G)$ denotes the **exponent** of $G$):

- The subnormal subgroups are exponential;
- $H$ is exponential if $|G : H|$ is a multiple of $\exp(G)$;
- being exponential is a transitive relation;
- the intersection of exponential subgroups is exponential.

The following is the key property of exponential subgroups:

**Lemma**

*Let $H \leqslant_{exp} G$ be core-free. Then $|G : H|$ is a multiple of $\exp(G)$.*

**Proof.**

Let $n = |G : H|$. Then $H$ contains the subgroup $G^n$ generated by the $n$-th powers. But $H$ is core-free and so $G^n = 1$. □

There exist non-subnormal exponential subgroups whose index is not a multiple of the exponent. A simple example is $G = C_4 \times \mathrm{Sym}(3)$ and $H \cong C_2 \times C_2$.

There exist non-subnormal exponential subgroups whose index is not a multiple of the exponent. A simple example is $G = C_4 \times \mathrm{Sym}(3)$ and $H \cong C_2 \times C_2$.

Sometimes the notion of being exponential collapses to that of being normal:

**Lemma**

- *If $H \leqslant_{exp} G$ is a Hall subgroup, then $H \lhd G$;*

There exist non-subnormal exponential subgroups whose index is not a multiple of the exponent. A simple example is $G = C_4 \times \mathrm{Sym}(3)$ and $H \cong C_2 \times C_2$.

Sometimes the notion of being exponential collapses to that of being normal:

### Lemma

- *If $H \leqslant_{exp} G$ is a Hall subgroup, then $H \lhd G$;*
- *If $G$ is solvable, and $H$ is exponential and maximal, then $H \lhd G$.*

There exist non-subnormal exponential subgroups whose index is not a multiple of the exponent. A simple example is $G = C_4 \times \mathrm{Sym}(3)$ and $H \cong C_2 \times C_2$.

Sometimes the notion of being exponential collapses to that of being normal:

## Lemma

- *If $H \leqslant_{exp} G$ is a Hall subgroup, then $H \lhd G$;*
- *If $G$ is solvable, and $H$ is exponential and maximal, then $H \lhd G$.*

**Remark:** We cannot drop the hypothesis of solvability in the second part: $G = \mathrm{Alt}(10)$ has a conjugacy class of maximal subgroups $H$ of size 720. Since $\exp(G) = 2520 = |G : H|$, it happens that $H$ is an exponential maximal subgroup which is not (sub)normal.

Recently, E. Swartz and N. Werner introduced the following:

### Definition

$G$ is **exp-simple** if its only proper exponential subgroups are those whose index is a multiple of $\exp(G)$.

Since all subgroups of a simple group are core-free, it is clear from above that the finite simple groups are exp-simple.

Recently, E. Swartz and N. Werner introduced the following:

**Definition**

$G$ is **exp-simple** if its only proper exponential subgroups are those whose index is a multiple of $\exp(G)$.

Since all subgroups of a simple group are core-free, it is clear from above that the finite simple groups are exp-simple.

They proved the following:

**Theorem (Swartz, Werner '25)**

*$G$ is exp-simple if and only if $\exp(G) = \exp(G/N)$ for all proper $N \lhd G$.*

The dream would be to find an elementary proof of the Kegel-Wielandt conjecture, in particular of

$$|HK| \text{ divides } |G| \text{ for all } K \leqslant G \quad \Longrightarrow \quad H \lhd \lhd G.$$

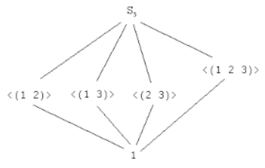
The dream would be to find an elementary proof of the Kegel-Wielandt conjecture, in particular of

$$|HK| \text{ divides } |G| \text{ for all } K \leqslant G \quad \Longrightarrow \quad H \lhd \lhd G.$$

More realistically, it would be interesting to know the exponential maximal subgroups of the finite simple groups. (These are the maximal subgroups whose index is a multiple of the exponent.)

*Computer experiments suggest they are rare:*

| $G$ | $\exp(G)$ | exponential maximal subgroups |
|---|---|---|
| $M_{12}$ | 1320 | $\mathrm{Alt}(4) \times \mathrm{Sym}(3)$ |
| $HJ$ | 840 | $\mathrm{Alt}(5),\ \mathrm{Alt}(5) \times \mathrm{Alt}(4)$ |
| $\mathrm{Alt}(10)$ | 2520 | $\mathrm{Alt}(6).C_2$ |
| $\mathrm{Alt}(15)$ | 360360 | $\mathrm{Alt}(8),\ \mathrm{Alt}(8)$ |
| $\mathrm{Alt}(16)$ | 360360 | $(C_2)^4.\mathrm{Alt}(8),\ (C_2)^4.\mathrm{Alt}(8)$ |




Thank you for your attention