# The First-Order Theory of Finite Groups

John Wilson

jsw13@cam.ac.uk; John.Wilson@maths.ox.ac.uk;
wilson@math.uni-leipzig.de

Gliwice, 11 September 2019

# Some ideas of finite group theory

- Proof by induction, minimal counter-examples
- nilpotence, solubility, simplicity
- Sylow theory, Hall theory for soluble groups
- maximal subgroups
- Frattini subgroup $\Phi(G)$ of $G = \bigcap$ (maximal subgroups of $G$)
- the subgroup generated by a subset.

**Theorem (Frattini, 1885).** For $G$ finite, $\Phi = \Phi(G)$ is nilpotent.
Proof. Let $P \in \mathrm{Syl}_p(\Phi)$. For each $g \in G$, $\exists f \in \Phi$ with $P^g = P^f$, and $gf^{-1} \in \mathrm{N}_G(P)$. So $G = \mathrm{N}_G(P)\Phi$. If $\mathrm{N}_G(P) < G$ find maximal $M$ with $\mathrm{N}_G(P) \leqslant M$. Then $G = \mathrm{N}_G(P)\Phi \leqslant M$, contradiction.

# First-order sentences/formulae

| | | |
|---|---|---|
| $(\forall x \forall y \forall z)([x,y,z]=1)$ | $G$ nilp. of class $\leqslant 2$ | Yes! |
| $(\forall x \in G')(\forall z)([x,z]=1)$ | $G$ nilp. of class $\leqslant 2$ | No! |
| $(\forall x_1 \forall x_2 \forall x_3 \forall x_4)(\exists y_1, y_2)([x_1,x_2][x_3,x_4]=[y_1,y_2])$ | every element of $G'$ is a commutator | |
| $(\forall x_1 \forall x_2 \exists y)(y \neq x_1 \wedge y \neq x_2)$ | $\lvert G\rvert \geqslant 3$ | |
| $(\forall x_1 \forall x_2 \forall x_3 \forall x_4)(\bigvee_{1\leqslant i<j\leqslant 4} x_i = x_j)$ | $\lvert G\rvert \leqslant 3$ | |
| $(\forall x)(x^6 = 1 \to x = 1)$ | no elements of order $2,3$ | |
| $g^4 = 1 \wedge g^2 \neq 1$ | $g$ has order 4 | |
| $(\exists n)(g^n = 1)$ | $g$ has finite order | No! |
| $(\forall x \in G')(x^7 = 1)$ | $G'$ has exponent dividing 7 | No! |
| $(\forall k \neq 1)(\forall g)(\exists r \in \mathbb{N})(\exists x_1, \ldots, x_r)(g = k^{x_1} k^{x_2} \ldots k^{x_r})$ | | No! |
| $(\forall x)(x^2 = 1 \to x = 1)$ | $\lvert G\rvert$ is odd (for finite $G$) | Yes! |

# Multiplication tables define finite groups

Let $H = \{h_1, \ldots, h_n\}$ be finite, set $h_i h_j = h_{\mu(i,j)}$.

Mult. table suggests formula

$\theta_H(x_1, \ldots, x_n)$: $(\bigwedge_{i \neq j}(x_i \neq x_j) \wedge \bigwedge_{i,j}(x_i x_j = x_{\mu(i,j)}))$.

Define

$\phi_H$: $(\exists x_1 \cdots \exists x_n)\, \theta_H(x_1, \ldots, x_n)$

$\psi_H$: $(\exists x_1 \cdots \exists x_n)(\forall y)(\theta_H(x_1, \ldots, x_n) \wedge (\bigvee_i y = x_i))$

$G \models \phi_H$: $\exists$ subgroup $\cong H$, $\qquad$ $G \models \psi_H$: $G \cong H$.

*Proof.* Multiplication table.

# Classes of finite groups defined by one sentence

($\exists$ only $\aleph_0$ such!)

(1) {groups of order $\leqslant n$}, {groups of order $\geqslant n$}, {groups with no elements of order $n$}

(2) Groups containing a copy of $A_6$ but not one of $A_7$, etc.

(3) Groups nilpotent of class $\leqslant c$; groups soluble of derived length $\leqslant d$

## Infinitely many sentences

$G$ is nilpotent: for all coprime integers $r, s > 1$ the sentence
$\forall x \forall y \ (x^r = y^s = 1 \to [x, y] = 1)$.

$G$ is soluble: for all coprime integers $r, s, t > 1$ the sentence
$\forall x \forall y \forall z \ (x^r = y^s = z^t = 1 \to x = 1)$.

simplicity?

# More classes of finite groups defined by one sentence

Soluble groups:

characterized by 'no $g \neq 1$ is a prod. of commutators $[g^h, g^k]$'; that is, $\rho_n$ holds $\forall n$

$$\rho_n : (\forall g \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n)(g = 1 \vee g \neq [g^{x_1}, g^{y_1}] \ldots [g^{x_n}, g^{y_n}]).$$

**Theorem (JSW 2005)** Finite $G$ is soluble iff it satisfies $\rho_{56}$.

# More classes of finite groups defined by one sentence

**Felgner's Theorem (1990).** $\exists$ sentence $\sigma$ (in the f.-o. language of group theory) such that, for $G$ finite, $G \models \sigma \Leftrightarrow G$ is non-abelian simple.

$\sigma = \sigma_1 \wedge \sigma_2$ with

$\sigma_1$: $(\forall x \forall y)(x \neq 1 \wedge \mathrm{C}_G(x,y) \neq \{1\} \rightarrow \bigcap_{g \in G} (\mathrm{C}_G(x,y)\mathrm{C}_G(\mathrm{C}_G(x,y)))^g = \{1\})$,
$\sigma_2$: 'each element is a product of $\kappa_0$ commutators' for a fixed $\kappa_0 \in \mathbb{N}$.

(Can now take $\kappa_0 = 1$ from verification of Oré conjecture:
all elements of non-abelian (finite) simple groups are commutators.)

$\sigma_1$ works as finite simple groups are 2-generator groups.

# More classes of finite groups defined by one sentence

A group $G$ is quasisimple if $G$ perfect and $G/\mathrm{Z}(G)$ simple

Proposition (JSW 2017) A finite group $G$ is quasisimple iff $Q$ satisfies $\mathrm{QS}_1 \wedge \mathrm{QS}_2 \wedge \mathrm{QS}_3$:

$\mathrm{QS}_1$: each element is a product of two commutators;
$\mathrm{QS}_2$: $(\forall x)(\forall u)[x, x^u] \in \mathrm{Z}(G) \to x \in \mathrm{Z}(G)$;
$\mathrm{QS}_3$:
$(\forall x \forall y)(x \notin \mathrm{Z}(G) \wedge \mathrm{C}_G(x,y) > \mathrm{Z}(G)) \to \bigcap_{g \in G} (\mathrm{C}_G(x,y)\mathrm{C}_G^2(x,y))^g = \mathrm{Z}(G)$.

($\mathrm{C}_G^2(X)$ stands for $\mathrm{C}_G\mathrm{C}_G(X)$.)

# Definable sets

... sets of elements $g \in G$ (or in $G^{(n)} = G \times \cdots \times G$) defined by first-order formulae, possibly with parameters from $G$.

Examples: • $Z(G)$, defined by $(\forall y)([x, y] = 1)$

• $r$th term $Z_r(G)$ of upper central series, defined by formula $\zeta_r$: $(\forall y_1, \ldots, y_r)([x, y_1, \ldots, y_r] = 1)$

• $C_G(h)$, defined by $[x, h] = 1$

• conjugacy class of $h$ defined by $(\exists y)\, x = h^y$

• Centralizers of definable sets are definable:
Say $S = \{s \mid \varphi(s)\}$; then $C_G(S) = \{t \mid \forall g(\varphi(g) \to [g, t] = 1)\}$

# Another definable set

Recall that sets like $\mathrm{Z}(G)$, $\mathrm{Z}_r(G)$, $\mathrm{C}_G(S)$ for $S$ definable are definable.

The (*soluble*) *radical* $\mathrm{R}(G)$ of a finite group $G$ is the largest soluble normal subgroup of $G$.

**Theorem (JSW 2008)** There's a f.-o. formula $r(x)$ such that if $G$ is finite and $g \in G$ then $g \in \mathrm{R}(G)$ iff $r(g)$ holds in $G$.

# What about nilpotency, $p$-groups?

Unfortunately there isn't a f.-o. sentence that holds in a finite group iff it's nilpotent.
Unfortunately there isn't a sentence saying that a finite group is a $p$-group.

So no Sylow theory. (Attempts have been made to reconstruct Sylow 2-subgroups, with no success yet.)

# More definable sets

- $X_h = \{[h^{-1}, h^g] \mid g \in G\}$, $\quad W_h = \bigcup\{X_{h^g} \mid g \in G, [X_h, X_{h^g}] \neq 1\}$.
- Centralizer of $S = \{s \mid \varphi(s)\}$ is $C_G(S) = \{t \mid \forall g(\varphi(g) \to [g,t] = 1)\}$.
- A useful idea: for definable $S \subseteq G$, defined by $\phi$, in general, $\langle S \rangle$ can't be defined in terms of $\phi$, but the bigger subgroup $C_G^2(S)$ can:
$\{g \mid \forall x((\forall s)(\phi(s) \to [s,x] = 1) \to [g,x] = 1)\}$.

So $\exists$ f.o. formula $\omega_h$ with $\omega_h(g)$ iff $g \in C_G^2(W_h)$
- $\delta(x,y)$: $\delta(h_1, h_2)$ iff $C_G^2(W_{h_1}) = C_G^2(W_{h_2})$

$\{(h_1, h_2) \mid \delta(h_1, h_2)\}$ definable in $G^{(2)}$, a definable equiv. relation
- $\exists\ \beta(x)$: $\beta(h)$ iff $C_G^2(W_h)$ commutes with its distinct conjugates.

$G$ finite: component = quasisimple subgroup $Q$ that commutes with its distinct $G$-conjugates ($\Leftrightarrow$ $Q$ subnormal).

**Theorem (JSW 2017)** $\exists$ f.o. formulae $\pi(h, y)$, $\pi'(h)$, $\pi'_{\mathrm{c}}(h)$, $\pi'_{\mathrm{m}}(h)$ such that for every finite $G$, the products of components of $G$ are the sets $\{x \mid \pi(h, x)\}$ for the $h \in G$ satisfying $\pi'(h)$.

The components: the sets $\{x \mid \pi(h, x)\}$ for which $\pi'_{\mathrm{c}}(h)$ holds.
The non-ab. min. normal subgps.: $\{x \mid \pi(h, x)\}$ with $\pi'_{\mathrm{m}}(h)$.

# Ultraproducts

Let $(G_i \mid i \in I)$ be an infinite family of groups.
An ultraproduct $U$ is a certain type of quotient of $C := \prod G_i$ (=Cartesian product containing all 'sequences' $(g_i)$ with $g_i \in G_i$), with the foll. property (Los' Theorem):
If $\theta$ a first-order sentence and $G_i \models \theta$ for all but finitely many $i$ then $U \models \theta$.

Similarly for ultraproducts $U$ of fields $F_i$. (First order in language of field theory–or ordered field theory if all $F_i$ are ordered fields.)
If all $F_i \cong \mathbb{R}$ then $U$ is a field containing $\mathbb{R}$ with infinitesimals:

**Corollary (A. Robinson, 1960s)** Calculus without limits (Leibniz' idea, ca. 1670).

An ultraproduct of finite groups of unbounded order is an infinite group satisfying all f.-o. sentences valid in all finite groups: something like a finite group with infinitesimals.

Some sentences valid for all finite groups

- $x \mapsto x^n$ injective iff $x \mapsto x^n$ surjective:
  $(\forall x_1 \forall x_2)(x_1^n = x_2^n \to x_1 = x_2) \leftrightarrow (\forall x \exists y)(x = y^n)$
- $C_G(x) \leqslant C_G(x^y) \to C_G(x) = C_G(x^y)$
- Higman:

$\langle x, y, z, w \mid x^y = x^2, y^z = y^2, z^w = z^2, w^x = w^2 \rangle$ is non-trivial but has no finite images $\neq 1$.

So finite groups satisfy

$(\forall a, b, c, d)(a^b \neq a^2 \vee b^c \neq b^2 \vee c^d \neq c^2 \vee d^a \neq d^2 \vee a = 1)$.

# Pseudo-finite (psf) groups

. . . infinite models for the theory of finite groups; i.e., infinite groups satisfying all first-order sentences valid in all finite groups.

Studied by **Felgner;** and later by me, Macpherson + Tent, and Ould-Houcine + Point, and others.

**Similarly psf fields.**

Psf examples. (1) Ultraproducts.

(2) If $K$ is a psf field, L a Lie type and if $G \equiv \mathrm{L}(K)$, then $G$ is simple psf. E.g. $\mathrm{PSL}_2(K)$ with $K$ psf.

**Theorem (JSW 1995 (+Ryten 2007)).** If G is simple psf then $G \cong \mathrm{L}(K)$ for some psf field $F$ and Lie type L.

A psf group $S$ is definably simple if $\nexists$ definable normal subgroups except $1, S$.

**Proposition (Felgner).** $G$ is definably simple iff $G \equiv$ an UP of finite simple groups.

An ultraproduct of $\{A_n \mid n \geqslant 5\}$ is definably simple but not simple.

Easy Fact. Let $I = I_1 \cup \cdots \cup I_r$. Then an ultraproduct of groups $G_i (i \in I)$ is isomorphic to an ultraproduct of groups $G_i (i \in I_j)$ for some $j$.

So in an ultraproduct of simple groups, can assume all or none of the groups are alternating.

# CFSG

Alternating groups: $\mathrm{Alt}(n),\ n \geqslant 5$;

Chevalley groups:

| Untwisted | Twisted |
| --- | --- |
| Classical | |
| $\mathrm{A}_n(q), \mathrm{B}_n(q), \mathrm{C}_n(q), \mathrm{D}_n(q)$ | ${}^2\mathrm{A}_n(q), {}^2\mathrm{D}_n(q)$ |
| Exceptional | |
| $\mathrm{E}_6(q), \mathrm{E}_7(q), \mathrm{E}_8(q), \mathrm{F}_4(q), \mathrm{G}_2(q)$ | ${}^2B_2(q), {}^3\mathrm{D}_4(q), {}^2\mathrm{G}_2(q), {}^2\mathrm{E}_6(q), {}^2\mathrm{F}_4(q)$ |

for some prime powers $q$ and integers $n \geqslant 1$;

26 sporadic groups.

# UPs of finite simple groups

From CFSG (together with Fact) any infinite ultraproduct $U$ of simple groups $G_i$ is isom. to one such that:

(a) $\forall i,\ G_i \cong \mathrm{Alt}(n_i)$, where $n_i \geqslant 5$; or

(b) $\forall i,\ G_i \cong {}^{\varepsilon}\mathrm{X}_{n_i}(q_i)$, where $\varepsilon \in \{1,2,3\}$ is fixed, $\mathrm{X} \in \{\mathrm{A},\mathrm{B},\ldots,\mathrm{G}\}$ is fixed, $n_i, q_i$ vary.

I showed that if also $U$ is simple then (a) can't arise and in (b) the $n_i$ are bounded. So can assume all $n_i$ equal.

(F. Point, 1999) For each Lie type L, any UP of groups of type L is a group of type L.

Any UP of finite simple groups of bounded rank is isom. to some $\mathrm{L}(K)$ and is psf. (As it's simple, it equals the corresponding metric UP.)

$G$ finite: component $=$ perfect subgroup $Q$ with $Q/\mathrm{Z}(Q)$ simple that commutes with its distinct $G$-conjugates ($\Leftrightarrow$ $Q$ subnormal).
$G$ psf: component $=$ definable 'perfect' subgroup $Q$ with $Q/\mathrm{Z}(Q)$ definably simple that commutes with its distinct conjugates.

If $G$ is psf, then $\mathrm{R}(G)$ and $G/\mathrm{R}(G)$ are psf or finite.

**Theorem (JSW 2017).** Let $G$ be $G$ psf.
(a) every non-trivial definable normal subgroup contains either a non-trivial abelian normal subgroup or a non-abelian minimal definable normal subgroup of $G$;
(b) each non-abelian minimal definable normal subgroup of $G$ is $S \times \mathrm{C}_G(S)$ for a definably simple component $S$;
(c) distinct components commute, so the product of finitely many such is definable;
(d) all non-abelian minimal normal subgroups and all products in (c) have the form $\{x \mid \pi(h, x)\}$ for elements $h \in G$, with $\pi$ as before.

# Pseudofinite definably simple groups

The simple ones: groups of Lie type over pseudofinite fields
Each non-simple one is associated with an infinite family of finite simple groups of unbounded rank of following kind:
alternating groups,
classical groups of even characteristic
classical groups of odd characteristic

In $A_n$ with $n \geqslant 8$ the normalizer $\mathrm{N}_{A_n}(\langle t_0 \rangle)$ for a 3-cycle $t_0 = (a, b, c)$ is the subgroup mapping $\{a, b, c\}$ to itself; it is maximal, and defined by the formula $t_0^x = t_0 \vee t_0^x = t_0^{-1}$.
Let $t \in A_n$ be a product of $r$ disjoint 3-cycles. Then $C = \mathrm{C}_{A_n}(t)$ contains a copy of $(\langle t \rangle \operatorname{wr} A_r) \times A_{n-3r}$ with index at most 2.
$|\{g \in C \text{ of order } 3 \mid g \text{ commutes with all its conjugates in } C\}| = 3^r - 1$.
So $t$ is a 3-cycle iff $A_n \models \tau(t)$:
$t \neq 1 \wedge t^3 = 1 \wedge (\forall u_1 u_2 u_3)(\bigwedge([u_i, t] = 1 \wedge [x, x^{u_i}] = 1) \to \bigvee_{i<j} x^{u_i} = x^{u_j}$.

So if $A_n \models \tau(t)$ then $\{g \mid \{g \mid t^g = t \vee t_g = t^{-1}\}$ is a maximal subgroup.
'Hence ...'

**Proposition.**
(a) If $G$ is (psf definably simple and) $\equiv$ an UP of groups $A_n$ and $G \models \tau(t)$ then $\{g \mid t^g = t \vee t^g = t^{-1}\}$ is a (definable!) maximal subgroup.
(b) (90%) Every psf definably simple group has a maximal definable subgroup (so $\bigcap$ (conjugates) $= 1$).

**Probably provable.** (70%) $\exists$ f.o. formulae $\mu(x,y), \nu(x)$ such that if $G$ is finite simple, large enough, and $G \models \nu(h)$ then $\{g \mid \mu(g,h)\}$ is a maximal subgroup.

**Conjecture.** $\exists$ f.o. formulae $\alpha(x,y)$, $\beta(x)$ such that for finite $G$
- $G \models \beta(h)$ implies that $\{g \mid \alpha(g,h)\}$ is a maximal subgroup;
- $\bigcap_{G \models \beta(h)} \{g \mid \alpha(g,h)\}$ is soluble.

(In particular, $\bigcap$ (maximal def. subgroups) would be soluble!)

**Probably provable.** (60%) $\exists$ f.o. formulae $\alpha(x,y)$, $\beta(x)$ such that for finite non-soluble $G$ if $h \in G$ and $G \models \beta(h)$ then $\{g \mid \alpha(g,h)\}$ is a maximal subgroup.

So any psf group is either pseudosoluble (satisfies $\sigma_{56}$) or has a maximal definable subgroup.

**Question.** Does every psf group have a maximal subgroup?

# What next for psf groups?

Note that psf $G$ is pseudo-(finite soluble) iff satisfies $\rho_{56}$, and same for definable subgroups.

Are there **any** (pseudo-)nilpotent def. subgroups that we can recognise?

- (Carter subgroups?)
- E.g. $L < H$, $L$ definable $\Rightarrow L < \mathrm{N}_H(L)$, def. normalizer condition for $H$
  But this requires a sentence for each definable subgroup.

Abelian normal subgroups in definable images, Clifford theory?

(Sabbagh.) Are there any finitely generated pseudofinite groups?