The First-Order Theory of Finite Groups

John Wilson

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

Ischia, 21 March 2018

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

$(\forall k \neq 1)(\forall g)(\exists r \in \mathbb{N})(\exists x_1, \ldots, x_r)(g = k^{x_1} k^{x_2} \ldots k^{x_r})$ simple No!

Classes of finite groups defined by a sentence

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

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

Classes of finite groups defined by a 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) **Felgner's Theorem (1990).** $\exists$ sentence σ (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

σ_1: $(\forall x \forall y)(x \neq 1 \wedge \mathrm{C}_G(x,y) \neq \{1\} \rightarrow \bigcap_{g \in G} (\mathrm{C}_G(x,y)\mathrm{C}_G(C_G(x,y)))^g = \{1\})$,
σ_2: 'each element is a product of κ_0 commutators' for a fixed $\kappa_0 \in \mathbb{N}$.

(In fact we can now take $\kappa_0 = 1$ from verification of Oré conjecture (finished by Liebeck, O'Brien, Shalev, Tiep, 2010):
all elements of non-abelian (finite) simple groups are commutators.)

σ_1 works as finite simple groups are 2-generator groups.

Ulrich Felgner

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 $\mathrm{QS}_1 \wedge \mathrm{QS}_2 \wedge \mathrm{QS}_3$:

QS_1: each element is a product of two commutators;
QS_2: $(\forall x)(\forall u)[x, x^u] \in \mathrm{Z}(G) \to x \in \mathrm{Z}(G)$;
QS_3:
$(\forall x \forall y)(x \notin \mathrm{Z}(G) \wedge \mathrm{C}_G(x,y) > \mathrm{Z}(G)) \to \bigcap_{g \in G}(\mathrm{C}_G(x,y)\mathrm{C}^2_G(x,y))^g = \mathrm{Z}(G)$.

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

Soluble groups:

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

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

Soluble groups:

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

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

Theorem (JSW 2005) Finite G is soluble iff it satisfies ρ_{56}.

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

• $\mathrm{C}_G(h)$, defined by $[x, h] = 1$

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

• $\mathrm{C}_G(h)$, defined by $[x, h] = 1$

• $X_h = \{[h^{-1}, h^g] \mid g \in G\}$, $\quad W_h = \bigcup\{X_{h^g} \mid g \in G, [X_h, X_{h^g}] \neq 1\}$.

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

• $\mathrm{C}_G(h)$, defined by $[x, h] = 1$

• $X_h = \{[h^{-1}, h^g] \mid g \in G\}$, $\quad W_h = \bigcup\{X_{h^g} \mid g \in G, [X_h, X_{h^g}] \neq 1\}$.

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

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

• $\mathrm{C}_G(h)$, defined by $[x, h] = 1$

• $X_h = \{[h^{-1}, h^g] \mid g \in G\}$, $\quad W_h = \bigcup\{X_{h^g} \mid g \in G, [X_h, X_{h^g}] \neq 1\}$.

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

So $\exists$ f.o. formula ω_h with $\omega_h(g)$ iff $g \in \mathrm{C}_G^2(W_h)$
• $\delta(x, y)$: $\delta(h_1, h_2)$ iff $\mathrm{C}_G^2(W_{h_1}) = \mathrm{C}_G^2(W_{h_2})$
$\{(h_1, h_2) \mid \delta(h_1, h_2)\}$ definable in $G^{(2)}$, a definable equiv. relation

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

• $\mathrm{C}_G(h)$, defined by $[x, h] = 1$

• $X_h = \{[h^{-1}, h^g] \mid g \in G\}$, $\quad W_h = \bigcup\{X_{h^g} \mid g \in G, [X_h, X_{h^g}] \neq 1\}$.

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

So $\exists$ f.o. formula ω_h with $\omega_h(g)$ iff $g \in \mathrm{C}^2_G(W_h)$
• $\delta(x, y)$: $\delta(h_1, h_2)$ iff $\mathrm{C}^2_G(W_{h_1}) = \mathrm{C}^2_G(W_{h_2})$
$\{(h_1, h_2) \mid \delta(h_1, h_2)\}$ definable in $G^{(2)}$, a definable equiv. relation
• $\exists$ $\beta(x)$: $\beta(h)$ iff $\mathrm{C}^2_G(W_h)$ commutes with its distinct conjugates.

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.

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 $\pi'_{\mathrm{m}}(h)$.

Lemma. Let M be a a product of some components Q_i of finite G, let $X \subseteq M$ have non-trivial projection in each $Q_i/\mathrm{Z}(Q_i)$. Then
(a) $M = \langle X^g \mid g \in M, [X, X^g] \neq 1\rangle$.

Chris Parker's nicer proof of (a).
$H := \langle X\rangle$. So $[X, X^g] \neq 1 \Leftrightarrow [H, H^g] \neq 1$.
$\langle H^g \mid g \in M\rangle \lhd M$, all projections $\neq 1$, so $\langle H^g \mid g \in M\rangle = M$. Let $K = \langle H^g \mid [H, H^g] \neq 1\rangle$.
$\mathrm{N}_M(H)$: contains the H^g that commute with H;
permutes the H^g that don't.
So $\mathrm{N}_M(H)$ normalizes K. Thus $\langle H^g \mid g \in M\rangle \leqslant \langle K, \mathrm{N}_M(H)\rangle = \mathrm{N}_M(H)K$ and $M = \mathrm{N}_M(H)K$.
$\exists\ g_0 \in M$ with $H^{g_0} \leqslant K$.
Let $g \in M$, let $g_0 = n_0k_0$, $g = nk$ with $n_0, n \in \mathrm{N}_M(H)$, $k_0, k \in K$.
Then $H^g = H^{nn_0^{-1}g_0k_0^{-1}k} = H^{g_0k_0^{-1}k} \leqslant K^{k_0^{-1}k} = K$.

For $h \in G$ define

$$X_h = \{[h^{-1}, h^g] \mid g \in G\} \quad \text{and} \quad W_h = \bigcup (X_h^f \mid f \in G, [X_h, X_h^f] \neq 1).$$

Lemma. Let M be a a product of some components Q_i of finite G, let $X \subseteq M$ have non-trivial projection in each $Q_i/\mathrm{Z}(Q_i)$. Then
(a) $M = \langle X^g \mid g \in M, [X, X^g] \neq 1 \rangle$.
(b) If also $[M, M^g] = 1$ whenever $M^g \neq M$ and $X = \{h\}$ then $M = \langle W_h \rangle$.
(a) $\Rightarrow$ (b) is easy.

Fact. If S is a component of a finite group G then $S \triangleleft \mathrm{C}_G^2(S)$.

Define δ_r for $r \geqslant 1$ recursively by $\delta_1(x_1, x_2) = [x_1, x_2]$ and
$\delta_r(x_1, \ldots, x_{2^r}) = [\delta_{r-1}(x_1, \ldots, x_{2^{r-1}}), \delta_{r-1}(x_{2^{r-1}+1}, \ldots, x_{2^r})]$ for $r > 1$.

Define δ_r for $r \geqslant 1$ recursively by $\delta_1(x_1, x_2) = [x_1, x_2]$ and $\delta_r(x_1, \ldots, x_{2^r}) = [\delta_{r-1}(x_1, \ldots, x_{2^{r-1}}), \delta_{r-1}(x_{2^{r-1}+1}, \ldots, x_{2^r})]$ for $r > 1$.

Begin with:

$$
\begin{aligned}
\varphi(h,x)&: \quad (\exists y)(x = [h^{-1}, h^y]) && \text{(defines } X_h\text{)}\\
\psi(h,x)&: \quad (\exists t \exists y_1 \exists y_2)(\varphi(h,y_1) \wedge \varphi(h^t, y_2) \wedge \varphi(h^t, x) \wedge\ [y_1, y_2] \neq 1) && \\
& && \text{(defines } W_h\text{)}\\
\gamma^1(h,x)&: \quad (\forall y)(\psi(h,y) \to [x,y] = 1) && \mathrm{C}_G(W_h)\\
\gamma(h,x)&: \quad (\forall y)(\gamma^1(h,y) \to [x,y] = 1) && \mathrm{C}_G^2(W_h)\\
\alpha^1(h,x)&: \quad (\exists y_1 \ldots \exists y_{16})\big(\big(\textstyle\bigwedge_{n=1}^{16} \gamma(h, y_n)\big) \wedge x = \delta_4(y_1, \ldots, y_{16})\big) && \\
& && \delta_4\text{-value in } \mathrm{C}_G^2(W_h)\\
\alpha(h,x)&: \quad (\exists y_1 \exists y_2)(\alpha^1(h,y_1) \wedge \alpha^1(h,y_1) \wedge x = y_1 y_2) &&
\end{aligned}
$$

Define δ_r for $r \geqslant 1$ recursively by $\delta_1(x_1, x_2) = [x_1, x_2]$ and
$\delta_r(x_1, \ldots, x_{2^r}) = [\delta_{r-1}(x_1, \ldots, x_{2^{r-1}}), \delta_{r-1}(x_{2^{r-1}+1}, \ldots, x_{2^r})]$ for $r > 1$.

Begin with:

$$\begin{aligned}
\varphi(h,x)&: \quad (\exists y)(x = [h^{-1}, h^y]) && \text{(defines } X_h\text{)}\\
\psi(h,x)&: \quad (\exists t \exists y_1 \exists y_2)(\varphi(h, y_1) \wedge \varphi(h^t, y_2) \wedge \varphi(h^t, x) \wedge \ [y_1, y_2] \neq 1) && \\
& && \text{(defines } W_h\text{)}\\
\gamma^1(h,x)&: \quad (\forall y)(\psi(h,y) \rightarrow [x,y] = 1) && \mathrm{C}_G(W_h)\\
\gamma(h,x)&: \quad (\forall y)(\gamma^1(h,y) \rightarrow [x,y] = 1) && \mathrm{C}_G^2(W_h)\\
\alpha^1(h,x)&: \quad (\exists y_1 \ldots \exists y_{16})(\big(\textstyle\bigwedge_{n=1}^{16} \gamma(h, y_n)\big) \wedge x = \delta_4(y_1, \ldots, y_{16})) && \\
& && \delta_4\text{-value in } \mathrm{C}_G^2(W_h)\\
\alpha(h,x)&: \quad (\exists y_1 \exists y_2)(\alpha^1(h, y_1) \wedge \alpha^1(h, y_1) \wedge x = y_1 y_2) &&
\end{aligned}$$

Let G be finite, Q a component. If $h \in Q \setminus \mathrm{Z}(Q)$ then $Q = \langle W_h \rangle$, so $Q \leqslant \mathrm{C}_G^2(W_h)$.
Show $Q =$ set of prods. of 2 δ_4-values in $\mathrm{C}_G^2(W_h)$, so $Q = \{x \mid \alpha(h,x)\}$.

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 θ a first-order sentence and $G_i \models \theta$ for all but finitely many i then $U \models \theta$.

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 θ 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).

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 θ 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.

Gottfried Wilhelm Leibniz (1646–1716), conceiver of infinitesimals, towering above us all

Some sentences valid for all finite groups

- $x \mapsto x^n$ injective iff $x \mapsto x^n$ surjective: $(\forall x_1 \forall x_2)(x_1^n = x_2^n \to x_1 = x_2) \leftrightarrow (\forall x \exists y)(x = y^n)$
- $\mathrm{C}_G(x) \leqslant \mathrm{C}_G(x^y) \to \mathrm{C}_G(x) = \mathrm{C}_G(x^y)$
- 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.

First studied by **Felgner;** further study by me, Macpherson + Tent, and Ould-Houcine + Point.

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.

First studied by **Felgner;** further study by me, Macpherson + Tent, and Ould-Houcine + Point.

Similarly psf fields.

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.

First studied by **Felgner;** further study by me, Macpherson + Tent, and Ould-Houcine + Point.

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.

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.

First studied by **Felgner;** further study by me, Macpherson + Tent, and Ould-Houcine + Point.

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.

Definably simple groups need not be simple

Proposition (Felgner). If $G \equiv$ an UP of $\{A_n \mid n \geqslant 5\}$ then G is definably simple but not simple.

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 π as before.

Theorem (JSW 2017). Let G be psf with $\mathrm{R}(G) = 1$ and with only finitely many components. Then G has a series

$$1 \leqslant G_1 \leqslant G_2 \leqslant G$$

of characteristic def. subgroups with G_1 the direct product of the components, G_2/G_1 metabelian, G/G_2 finite.

Similar ideas (X_h, W_h, double centralizers) used for

branch groups (JSW 2015): ambient tree is often (first-order-) interpretable in the branch group

right-ordered permutation groups (Andrew Glass, JSW 2016):

$\mathrm{Aut}_{\leqslant}(\Lambda) :=$ group of order-preserving permutations of ordered set Λ.

If $\mathrm{Aut}_{\leqslant}(\Lambda)$ is f.-o.-equivalent (for group language) to $\mathrm{Aut}_{\leqslant}(\mathbb{R})$ then Λ is isomorphic (as ordered set) to $\mathbb{R}$.

What next for psf groups?

Abelian normal subgroups in definable images, Clifford theory?

Big problem: no Sylow theory. Maybe exists for $p = 2$ using structure of dihedral groups? (Altinel, Borovik, Cherlin?)

psf G is pseudo-(finite soluble) iff satisfies ρ_{56}, same for def. subgroups.

How to recognise (pseudo-)nilpotent def. subgroups H?
E.g. $L < H$, L definable $\Rightarrow L < \mathrm{N}_H(L)$, def. normalizer condition for H???

(Carter subgroups?)

Is the Frattini subgroup pseudo-nilpotent?