Working effectively with generic subgroups

François Garillot

Microsoft Research–INRIA Joint Centre
Orsay, France

Working effectively with generic subgroups

François Garillot

work in progress

Microsoft Research–INRIA Joint Centre
Orsay, France

Classifying (some) simple finite groups

$\forall n \neq 1$, there exists a sequence

$$n = n_0 \geq n_1 \geq n_2 \geq \ldots \geq \ldots n_{r-1} \geq n_r = 1$$

such that n_i/n_{i+1} is **prime**, and that sequence of primes and their multiplicity are unique for each n.

Classifying (some) simple finite groups

$\forall n \neq 1$, there exists a sequence

$$n = n_0 \geq n_1 \geq n_2 \geq \ldots \geq \ldots n_{r-1} \geq n_r = 1$$

such that n_i/n_{i+1} is **prime**, and that sequence of primes and their multiplicity are unique for each n.

(Jordan-Hölder)
Given a finite group G, there exists a sequence

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_{r-2} \supset G_{r-1} \supset G_r = \{1\}$$

such that $G_{i+1} \lhd G_i$, G_i/G_{i+1} is **simple**, and that *composition series* is unique up to isomorphism and permutation.

The Feit-Thompson theorem

Finite groups of odd order are solvable.

Abel prize in 2008

Feit, Walter; Thompson, John G. , *Solvability of groups of odd order* ,

Pacific Journal of Mathematics 13: 775-1029 , 1963

The Feit-Thompson theorem

Finite groups of odd order are solvable.

Every goup of odd order has a composition series made of (simple) cyclic groups of prime order.

Abel prize in 2008

Feit, Walter; Thompson, John G. , *Solvability of groups of odd order* , Pacific Journal of Mathematics 13: 775-1029 , 1963

The Feit-Thompson theorem

Finite groups of odd order are solvable.

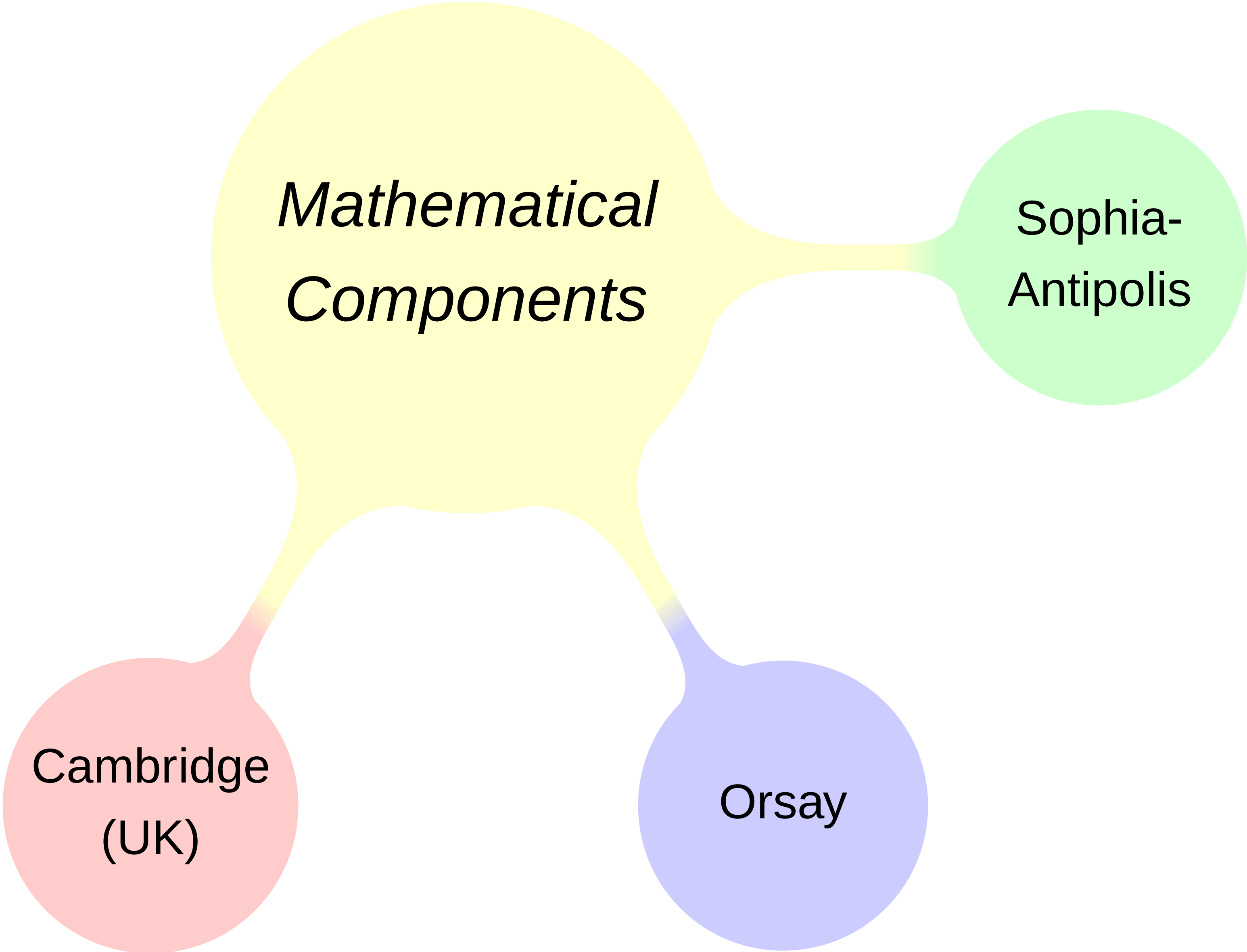
Every goup of odd order has a composition series made of (simple) cyclic groups of prime order.

Abel prize in 2008

Feit, Walter; Thompson, John G. , *Solvability of groups of odd order* , Pacific Journal of Mathematics 13: 775-1029 , 1963

254 pages !

One team, several locations



Characteristic groups

the set G, $\bullet : G \times G \to G$

+ *associativity, identity, inverse*

A **subgroup** H of a group G is a **characteristic subgroup** of G if $H^{\varphi} = H$ for all $\varphi \in \mathrm{Aut}(G)$.

Bijective morphisms of $G \to G$

Subgroups defined by functorials

Let F be a function from groups to groups that returns a specific subgroup,

$$F : G \mapsto H$$

We want

$$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} = F(G \quad)$$

Subgroups defined by functorials

Let F be a function from groups to groups that returns a specific subgroup,

$$F : G \mapsto H$$

We want

$$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} = F(G^{\varphi})$$

Formalized Groups

finGroupType

- `T :` Type, with decidable equality and finite enumeration
- `* : T -> T -> T`
- `1 : T`
- `_^-1 : T -> T`
- associativity, unit, inverse properties

Details : TPHOLS 2009!

Formalized Groups

{group gT}

- a **set** S : an indicator function on the enumeration of gT.
- closure of $*$ w.r.t. S
- $1 \in$ S

finGroupType

- T : Type, with decidable equality and finite enumeration
- `* : T -> T -> T`
- `1 : T`
- `_^-1 : T -> T`
- associativity, unit, inverse properties

Details : TPHOLS 2009!

Subgroups defined by functorials

$$F : \forall gT, \{group\, gT\} \to \{group\, gT\}$$

Example:

```
Definition Frattini (A:set gT): set gT :=
  \bigcap_(G : group gT | maximal_eq G A) G.

Canonical Structure Frattini_group A : group gT :=
  Eval hnf in [group of Frattini A].
```

We require

$$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} \subset F(G\quad)$$

Subgroups defined by functorials

$$F : \forall gT, \{group\, gT\} \to \{group\, gT\}$$

Example:

```
Definition Frattini (A:set gT): set gT :=
  \bigcap_(G : group gT | maximal_eq G A) G.

Canonical Structure Frattini_group A : group gT :=
  Eval hnf in [group of Frattini A].
```

We require

$$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} \subset F(G^{\varphi})$$

Subfunctors defined by functorials

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "F"] & H \arrow[d, "F"] \\ F(G) & F(H) \end{tikzcd}$$

gFunc

- $F : \forall gT, \{groupgT\} \rightarrow \{groupgT\}$
- $\forall G, F(G) \subset G$
- $\forall \varphi \in Aut(G)$, $F(G)^{\varphi} \subset F(G^{\varphi})$

Subfunctors defined by functorials

In **Grp** with arrows restricted to isomorphisms, F is the obj. mapping of a subfunctor $\mathcal{F}$ of I iff

$$F(G)^{\varphi} \subset F(H)$$

Then, $\mathcal{F}\varphi = \varphi|_{F(G)}$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "F"] & H \arrow[d, "F"] \\ F(G) \arrow[r, "\varphi|_{F(G)}"] & F(H) \end{tikzcd}$$

gFunc

- $F \ : \ \forall gT, \{groupgT\} \to \{groupgT\}$
- $\forall G, F(G) \subset G$
- $\forall \varphi \in \mathrm{Aut}(G)$, $F(G)^{\varphi} \subset F(G^{\varphi})$

Instances

L	Φ	$Z(G)$	O_p
J	G'	$F(G)$	O_π
$\mho_p$	$L_{(n)}$	$F^*(G)$	
Ω_p	$G^{(n)}$	$U_{(n)}$	

(plus some deprived of a nice notation)

How are (some of) these cases handled ?

1.23. Let x and y in F have m and n conjugates, respectively, in G. For each $u \in G$, $u^{-1}x^{-1}u = (u^{-1}xu)^{-1}$ and $u^{-1}(xy)u = (u^{-1}xu)(u^{-1}yu)$. Thus x^{-1} and xy have at most m and mn conj… F is a subgroup of G. Similarly, for … the same number of conjugates as x. … group (see [22]).

Theorem 5.21. *For every group G, the higher commutator subgroups are characteristic, hence normal subgroups.*

Proof. The proof is by induction on $i \geq 1$. Recall that the commutator subgroup $G' = G^{(1)}$ is generated by all commutators; that is, by all elements of the form $aba^{-1}b^{-1}$. If φ is an automorphism of G, then $\varphi(aba^{-1}b^{-1}) =$ $\varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$ is also a commutator, and so $\varphi(G') \leq G'$. For the in… …at $G^{(i+1)}$ char $G^{(i)}$; since $G^{(i)}$ char G, by … $G^{(i+1)}$ is characteristic in G. ∎

characteristic subgroups of G. Another example of a characteristic subgroup is $Z(G)$. Indeed, for $x \in Z(G)$, $g \in G$, $\alpha \in \operatorname{Aut} G$,

$$x^\alpha g^\alpha = (xg)^\alpha = (gx)^\alpha = g^\alpha x^\alpha,$$

and since $G = \{g^\alpha \mid g \in G\}$ we have $x^\alpha \in Z(G)$.

a Hierarchy of subfunctors

I

$$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} \subset F(G^{\varphi})$$

II

$$\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$$

III $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \rightarrow F(H) \leq F(G)$

IV $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \rightarrow F(G) \cap H \leq F(H)$

a Hierarchy of subfunctors

I

$\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} \subset F(G^{\varphi})$

II

$\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

III $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \to F(H) \leq F(G)$

$F \circ F'(G) = F(F'(G))$

IV $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \to F(G) \cap H \leq F(H)$

$F \circ F'(G) = (\_/F'(G))^{-1} F(G/F'(G))$

a Hierarchy of subfunctors

I $\forall \varphi \in \mathrm{Aut}(G), F(G)^{\varphi} \subset F(G^{\varphi})$

II $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

III $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \to F(H) \leq F(G)$

$F \circ F'(G) = F(F'(G))$

4

IV $\forall \varphi, F(G)^{\varphi} \subset F(G^{\varphi})$

$H \leq G \to F(G) \cap H \leq F(H)$

$F \circ F'(G) = (\_/F'(G))^{-1} F(G/F'(G))$

9

1

2

Subfunctors for finite group theory

- Simpler characteristicity proofs for everyone.
- Simple additional algebraic properties.

Subfunctors for finite group theory

- Simpler characteristicity proofs for everyone.
- Simple additional algebraic properties. *e.g.* :

$$\forall \mathsf{F} \in \mathsf{IV}, \mathsf{F} \circ \mathsf{F} = \mathsf{F}$$

Subfunctors for finite group theory

- Simpler characteristicity proofs for everyone.
- Simple additional algebraic properties. *e.g.* :

$$\forall \mathsf{F} \in \mathsf{IV}, \mathsf{F} \circ \mathsf{F} = \mathsf{F}$$

- Better compositionality than characteristic subgroups.

Subfunctors for finite group theory

- Simpler characteristicity proofs for everyone.
- Simple additional algebraic properties. *e.g.* :

$$\forall F \in \mathsf{IV}, F \circ F = F$$

- Better compositionality than characteristic subgroups. *e.g.*:If φ surjective,

$$H \,\mathrm{char}\, G \not\Rightarrow H^{\varphi} \,\mathrm{char}\, G^{\varphi}$$

$$F(G)^{\varphi} = F(G^{\varphi}) \,\mathrm{char}\, G^{\varphi}$$

Expressing parametricity ?

- still have to prove $\forall \varphi \in \mathrm{Aut}(G'), F(G)^{\varphi} = F(G^{\varphi})$
- Cayley (regular) representation of groups:

$$a \in G \rightsquigarrow (x \mapsto a \bullet x) \in \mathrm{perm}(G)$$

$$G \rightleftharpoons^{\psi}_{\psi^{-1}} G_p : \{\mathrm{group}(\mathrm{permI}_{|G|})\}$$

- Define functors as monomorphic on the Cayley representation. Define a uniform mapping of elements of gT to the Cayley representation.