Mechanizing the Odd Order Theorem: Local Analysis
In honour of Gérard Berry and Jean-Jacques Lévy

Assia Mahboubi

INRIA Microsoft Research Joint Centre (France)
INRIA Saclay – Île-de-France
École Polytechnique, Palaiseau

February 8, 2011
Finite group theory

Groups are algebraic structures closed under an associative, invertible law.
Finite group theory

Elements of a group combine thanks to the group law:

\[ g \quad g^{-1} \quad e \quad g \ast h \quad g \ast h \ast g^{-1} \]
Elements of a group combine thanks to the group law:

\[ g, g^{-1}, e, g \ast h, g \ast h \ast g^{-1} \]

But groups themselves combine through various kinds of operators:

\[ G \ltimes H, G \ast H, G \cap H, G \ltimes H, G/H \]
Finite group theory

- Elements of a group combine thanks to the group law:
  \[ g \quad g^{-1} \quad e \quad g \ast h \quad g \ast h \ast g^{-1} \]

- But groups themselves combine through various kinds of operators:
  \[ G \times H \quad G \ast H \quad G \cap H \quad G \rtimes H \quad G/H \]

- And most of the theory is developed forgetting about the points.
Decomposition

Theorem (Existence of prime decomposition)

A number always admits a decomposition into a product of prime numbers.

Theorem (Existence of composition series)

For any finite group $G$, there exists a sequence of subgroups:

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G = G_n$$

such that for all $k$, $G_{k+1}/G_k$ is simple.
Decomposition

Theorem (Existence of prime decomposition)

A number always admits a decomposition into a product of prime numbers.

Theorem (Existence of composition series)

For any finite group $G$, there exists a sequence of subgroups:

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G = G_n$$

such that for all $k$, $G_{k+1}/G_k$ is simple.

Such a sequence is called a composition series for $G$.  
Such a quotient $G_{k+1}/G_k$ is called a factor.
Uniqueness

Theorem (Prime decomposition uniqueness)

The decomposition of any number into a product of primes is unique up to permutations.

Theorem (Jordan-Hölder uniqueness)

For any group $G$, two composition series for $G$ have the same length, and the same factors up to isomorphism and permutation.
Proving Jordan Hölder Theorem

By induction on the cardinal of $G$:
Proving Jordan Hölder Theorem

By induction on the cardinal of \( G \):
- **Base case**: \( \#G = 0 \).
  - trivial (a group has at least one element: the neutral)
Proving Jordan Hölder Theorem

By induction on the cardinal of $G$:

- **Base case:** $\#G = 0$.
  - trivial (a group has at least one element: the neutral)

- **Inductive case:** $\#G > 0$:
  - If $G$ has an empty series: then it is trivial and all its series are empty.
  - If $G$ is simple: then all its series are trivial.
  - Else let $(N_i)$ and $(M_j)$ be two (non empty) composition series of $G$. 

A. Mahboubi (INRIA)
Jordan Hölder Theorem

By induction on the cardinal of $G$:

$N_1 \rightarrow N_2 \rightarrow \ldots \rightarrow N_r = 1$

$M_1 \rightarrow M_2 \rightarrow \ldots \rightarrow M_s = 1$
By induction on the cardinal of $G$:

\[ I = N_1 \cap M_1 \]

\[ M_2 \]

\[ N_2 \]

\[ \ldots \]

\[ \ldots \]

\[ N_r = 1 \]

\[ M_s = 1 \]
Jordan H"{o}lder Theorem

By induction on the cardinal of $G$:

$I = N_1 \cap M_1$

$M_2 \triangleright \ldots \triangleright M_s = 1$

$N_2 \triangleright \ldots \triangleright N_r = 1$
Jordan Hölder Theorem

By induction on the cardinal of $G$:

$I = N_1 \cap M_1$

$N_2 \quad \ldots \quad N_r = 1$

$M_2 \quad \ldots \quad M_s = 1$
Jordan Hölder Theorem

By induction on the cardinal of $G$:

$$G = \bigcap_{i=1}^{t} N_i \cap M_i$$

$$I = N_i \cap M_i \quad \ldots \quad I_t = 1$$

$$M_2 \quad \ldots \quad M_s = 1$$
Jordan Hölder Theorem

By induction on the cardinal of $G$:

By induction hypothesis

$G$

$I = N_1 \cap M_1$  ......  $I_t = 1$

$M_2$  ......  $M_s = 1$

$N_2$  ......  $N_r = 1$
Jordan Hölder Theorem

By induction on the cardinal of \( G \):

\[
\text{Induction hypothesis}
\]

\[
N_2 \quad \Rightarrow \quad N_t = 1
\]

\[
I = N_1 \cap M_1 \quad \Rightarrow \quad I_t = 1
\]

\[
M_2 \quad \Rightarrow \quad M_s = 1
\]
Jordan Hölder Theorem

By induction on the cardinal of \( G \):

\[
\begin{align*}
N_1 & \implies N_2 \implies \cdots \implies N_t = 1 \\
M_1 & \implies I = N_1 \cap M_1 \implies \cdots \implies I_t = 1 \\
M_2 & \implies \cdots \implies M_s = 1
\end{align*}
\]
By induction on the cardinal of $G$:

$$\begin{align*}
N_2 & \quad \Rightarrow \quad N_t = 1 \\
N_1 & \quad \Rightarrow \quad I = N_1 \cap M_1 \quad \Rightarrow \quad I_t = 1 \\
G & \quad \Rightarrow \quad M_2 \quad \Rightarrow \quad M_t = 1
\end{align*}$$
Jordan Hölder Theorem

We have obtained:

\[ G \]

\[ I = N_1 \cap M_1 \quad \Rightarrow \quad N_t = 1 \]

\[ M_2 \quad \Rightarrow \quad M_t = 1 \]
Jordan Hölder Theorem

We have obtained:

\[ G \]

\[ N_1 \]

\[ M_1 \]

\[ I = N_1 \cap M_1 \]

\[ \ldots \]

\[ \Rightarrow N_t = 1 \]

\[ I_t = 1 \]
Jordan Hölder Theorem

We have obtained:

\[ I = N_1 \cap M_1 \implies \ldots \implies I_t = 1 \]
Jordan Hölder Theorem

We conclude by a “butterfly lemma”:

\[ I = N_1 \cap M_1 \quad \Rightarrow \quad \ldots \quad \Rightarrow \quad I_t = 1 \]
Finite group decomposition (continued)

Unfortunately the analogy with arithmetics soon breaks down:
Unfortunately the analogy with arithmetics soon breaks down:

- Two numbers with the same multiset of prime factors are equal.
Unfortunately the analogy with arithmetics soon breaks down:

- Two numbers with the same multiset of prime factors are equal.
- Two groups with the same (up to isomorphism) multiset of prime factors are not necessarily equal (not even isomorphic).
Unfortunately the analogy with arithmetics soon breaks down:

- Two numbers with the same multiset of prime factors are equal.
- Two groups with the same (up to isomorphism) multiset of prime factors are not necessarily equal (not even isomorphic).

⇒ Classifying finite groups is much more difficult than “classifying” numbers.
The Atlas of Finite Groups

The classification of all simple finite groups aka. The Enormous Theorem

has been considered achieved in 1983 and revised in 2005.
The Odd Order Theorem

Theorem (Feit - Thompson (1963)):

Every simple group of odd order is solvable. 

otherwise said

Every simple group of odd order is cyclic.
The Odd Order Theorem

Theorem (Feit - Thompson (1963)):

Every simple group of odd order is solvable.

*otherwise said*

Every simple group of odd order is cyclic.

- Original published proof: one entire volume of the Pacific Journal of Mathematics
The Odd Order Theorem

Theorem (Feit - Thompson (1963)):

Every simple group of odd order is solvable. *otherwise said*
Every simple group of odd order is cyclic.

- Original published proof: one entire volume of the Pacific Journal of Mathematics
The Odd Order Theorem

Theorem (Feit - Thompson (1963)) :

Every simple group of odd order is solvable.

*otherwise said*

Every simple group of odd order is cyclic.

- Original published proof: one entire volume of the Pacific Journal of Mathematics
- *(Wikipedia 01/02/2011)* “It takes a professional group theorist about a year of hard work to understand the proof completely.”
The Odd Order Theorem

Theorem (Feit - Thompson (1963)):

Every simple group of odd order is solvable. 

*otherwise said*

Every simple group of odd order is cyclic.

- Original published proof: one entire volume of the Pacific Journal of Mathematics
- (Wikipedia 01/02/2011) “It takes a professional group theorist about a year of hard work to understand the proof completely.”
- The proof mixes many theories, non only combinatorics but also linear algebra, Galois theory, characters,...
Formalization issues: sets vs. types

Not all distinct sets should be modelled as distinct types

- A type fixes common requirements for its inhabitants.
- Type inhabitants are objects we want to observe and combine.
Formalization issues: sets vs. types

Types should have the appropriate granularity.
Formalization issues: sets vs. types

Types should have the appropriate granularity. Remember the main objects we manipulate most are groups, not elements:
Formalization issues: sets vs. types

Types should have the appropriate granularity. Remember the main objects we manipulate most are groups, not elements:

\[
G \times H \quad G \ast H \quad G \cap H \quad G \ltimes H \quad G/H
\]
Formalization issues: sets vs. types

Types should have the appropriate granularity. Remember the main objects we manipulate most are groups, not elements:

\[ G \times H \quad G \ast H \quad G \cap H \quad G \ltimes H \quad G/H \]

- Work within a finite group domain type which fixes the law.
  
  \[ gT : \text{finGroupType} \]
Formalization issues: sets vs. types

Types should have the appropriate granularity. Remember the main objects we manipulate most are groups, not elements:

\[ G \times H \quad G \ast H \quad G \cap H \quad G \ltimes H \quad G/H \]

- Work within a finite group domain type which fixes the law.
  \[ \text{gT : finGroupType} \]
- Groups are collections (subsets) of inhabitants of this big group.
  \[ \text{G H : \{group gT\}} \]
Formalization issues: sets vs. types

Types should have the appropriate granularity.
Remember the main objects we manipulate most are groups, not elements:

\[ G \times H \quad G \ast H \quad G \cap H \quad G \rtimes H \quad G / H \]

- Work within a finite group domain type which fixes the law.
  \[ gT : \text{finGroupType} \]
- Groups are collections (subsets) of inhabitants of this big group.
  \[ G \ H : \{ \text{group } gT\} \]
- Operations on groups remain homogeneous.
Formalization issues: sets vs. types

Types should have the appropriate granularity. Remember the main objects we manipulate most are groups, not elements:

\[
G \times H \quad G \ast H \quad G \cap H \quad G \ltimes H \quad G / H
\]

- Work within a **finite group domain type** which fixes the law.
  
  \[
  gT : \text{finGroupType}
  \]

- Groups are collections (subsets) of inhabitants of this big group.
  
  \[
  G H : \{\text{group } gT\}
  \]

- Operations on groups remain homogeneous.

- Only change type when a new group law is really needed

  quotient groups...
Formalisation issues: notations

Let $M \in M_n(F)$,

$$\det(M) := \sum_{s \in S_n} (-1)^{\epsilon_s} \prod_i M_{i, s(i)}$$
Formalisation issues: notations

Let $M \in M_n(F)$,

$$\det(M) := \sum_{s \in S_n} (-1)^{\epsilon_s} \prod_i M_{i,s(i)}$$

In \LaTeX:

$$\det(M) := \sum_{s \in S_n} (-1)^{\epsilon_s} \prod_i M_{i,s(i)}$$

A. Mahboubi (INRIA)
Formalisation issues: notations

Let $M \in M_n(F)$,

$$\det(M) := \sum_{s \in S_n} (-1)^{\epsilon_s} \prod_{i} M_{i,s(i)}$$

In **\LaTeX**:

$$\det(M) := \sum_{s \in S_n} (-1)^{\epsilon_s} \prod_{i} M_{i,s(i)}$$

In a **proof assistant**, one would like to write:

**Definition** determinant n (A : 'M[R]_n) : R :=

$$\sum_{(s : 'S_n)} (-1)^{\epsilon_s} \prod_{i} A(i,s(i)).$$
Formalisation issues: notations

\[ \Sigma \quad \Pi \quad \bigcup \quad \bigcap \quad \oplus \ldots \]

This requires:

- Concise and uniform notations: \( \sum_{i=0}^{n} \bigcup A \notin E \bigcap A|P(A) \ldots \)
- Generic toolkit: \( \bigcap_{A \in E} \bigcap_{A \in E \cap B} \bigcap_{A \in E \cap B^c} \ldots \)
- Implicit properties of associated operators:

\[ \prod_{i=1}^{n} \sum_{j=1}^{m} = \sum \prod \]

This is possible using:

- A generic operator to program these expressions;
- Higher order type inference (à la type classes);
- Coq notation mechanism.
Formalization issues: a page in finite group theory

Finite groups, vol 2. VIII.5.9 - Huppert Blackburn (excerpt):

Since \( A/U = (K/U)(B/U) \), it follows that:

\[ A = KB = DB = DB \]

Also \( K \cap B = U \) and \( U^p(K) \cap D = U^p(K) \), so

\[ D \cap B = D \cap K \cap B = D \cap U = D \cap U^p(K) \cap U = U^p(K) \cap U = 1 \]

Thus \( A = D \times B \). Then \( K = D \times (B \times K) = D \times U \), so \( D \simeq K/U \) is homocyclic and \( D/\Phi(D) \) is \( K \)-irreducible. Also \( D \neq 1 \) so the inductive hypothesis may be applied to \( B \) and the theorem follows at once.
Formalization issues: a page in finite group theory

Fortunately a computer scientist is used to $\alpha$-conversion:

Since $A/U = (K/U)(B/U)$, it follows that:

$$A = KB = DUB = DB$$

Also $K \cap B = U$ and $U\bar{\mathcal{p}}(K) \cap D = \bar{\mathcal{p}}(K)$, so

$$D \cap B = D \cap K \cap B = D \cap U = D \cap U\bar{\mathcal{p}}(K) \cap U = \bar{\mathcal{p}}(K) \cap U = 1$$

Thus $A = D \times B$. Then $K = D \times (B \times K) = D \times U$, so $D \simeq K/U$ is homocyclic and $D/\Phi(D)$ is $X$-irreducible. Also $D \neq 1$ so the inductive hypothesis may be applied to $B$ and the theorem follows at once.
Yet as usual, the devil is in the details:

Since $A/U = (K/U)(B/U)$, it follows that:

$$A = KB = DUB = DB$$

Also $K \cap B = U$ and $U\mathcal{U}^p(K) \cap D = \mathcal{U}^p(K)$, so

$$D \cap B = D \cap K \cap B = D \cap U = D \cap U\mathcal{U}^p(K) \cap U = \mathcal{U}^p(K) \cap U = 1$$

Thus $A = D \times B$. Then $K = D \times (B \times K) = D \times U$, so $D \simeq K/U$ is homocylic and $D/\Phi(D)$ is $X$-irreducible. Also $D \neq 1$ so the inductive hypothesis may be applied to $B$ and the theorem follows at once.