What do we expect of a proof ?
The example of the simplicity of the alternating group

Antoine Chambert-Loir (*Université Paris Cité*)

15th French PhilMath Workshop
Paris, 18–20 October 2023

Abstract

Building on the example of a classic theorem in the group theory corpus, the simplicity of the alternating group on at least 5 letters, I would like to discuss the following question : **what do we expect of a proof ?** In particular, according to when we learn it, teach it, or write it. And when we write it, in what respect does the material that hosts that proof makes a difference, from a draft, a lectures syllabus, a reference monograph, a digital library of formal proofs.

More mathematical content can be found in my paper "Formalizing the proof of an intermediate-level algebra theorem – An experiment", `https://arxiv.org/abs/2303.12404`.

Summary

Simplicity of the alternating group

Theorem

Let n be an integer, $n \geqslant 5$. The alternating group $\mathfrak{A}_n$ is a simple group.

Simplicity of the alternating group

Theorem

Let n be an integer, $n \geqslant 5$. The alternating group $\mathfrak{A}_n$ is a simple group.

Reminder on definitions :

- The **alternating group** $\mathfrak{A}_n$ is the group of permutations $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ which have signature $+1$ — equivalently : products of an even number of transpositions (i, j).
- A group is **simple** if it is nontrivial and if its only normal subgroups are $\{1\}$ and itself. Morally : cannot be build out of two simpler groups.

Normal subgroups and simple groups

Another reminder :

- A subgroup H of a group G is **normal** if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$ — equivalently, there is an equivalence relation on G which is compatible with the group structure and such that H is the class of 1.

"Obvious" normal subgroups of a group G :

- The trivial subgroup $\{1\}$ and the group G itself ;
- If the group G is commutative, all of its subgroups are normal ;
- The center $Z(G)$ of G : elements h such that $gh = hg$ for all $g \in G$;
- The derived subgroup G', generated by all commutators $ghg^{-1}h^{-1}$.

Galois's theory of polynomial equations

The notion of "normal" subgroup is due to Galois (1830), in relation with the question of solvability by radicals and his own solution to that problem, solved by Abel (1824) after a partial solution by Ruffini (1799/1813).

Galois talks of « **décomposition propre** » and is interested in cases where the group of a polynomial equation is ultimately built of commutative groups (we now call such a group **solvable**), because then the solutions of the equation can be expressed using radicals only.

Noncommutative simple groups are not solvable, so that the solutions of an equation of degree n with group $\mathfrak{A}_n$, with $n \geqslant 5$, can't be expressed by radicals.

Jordan's treaty on permutation groups

The simplicity theorem is attributed to Galois, at least for $n = 5$.

Cayley (1854). Definition of an abstract group

Jordan (1870), **Traité des substitutions et des équations algébriques**. General systematic study (« développer les méthodes de Galois et les constituer en corps de doctrine ») of groups acting on sets.

The simplicity theorem appears early (§85) as a consequence of more general results that a subgroup of the symmetric group $\mathfrak{S}_n$ that acts "a lot" automatically contains the alternating group.

The Classification of Finite Simple Groups

In the second half of the 20th century, mathematicians managed to establish a complete classification of the **finite simple groups**. They come up in 4 sorts :

- Finite cyclic groups of prime orders ;
- The alternating groups $\mathfrak{A}_n$, for $n \geqslant 5$;
- Groups of geometric origin, defined using linear algebra — such as $\mathrm{PSL}(n, F)$ for a finite field F (of cardinality $\geqslant 4$ if $n = 2$) ;
- "Sporadic groups", a list of 26 groups with a mostly combinatorial definition, starting with M_{11}, M_{12} defined by Mathieu (1861) to J_4 defined by Janko (1974) and the Griess–Fischer **Monster**, whose existence and uniqueness was proved around 1980.

The Classification of Finite Simple Groups

The proof of the classification of the finite simple groups is tantalizingly **huge** : tens of thousands of pages, several hundreds of papers, more than 100 authors ; with a revision (1994) and a recent update (2008) fixing a mistake discovered in 1979.

It had (sometimes immediate) applications to some conjectures that are easily reducible to the case of finite simple groups and amenable to a case by case study. (For example, Zelmanov's proof of the "restricted Burnside problem" uses the classification.)

It is likely that its proof contains some incorrections, and some mathematicians are reluctant to use it. However, it is unlikely that these incorrections could lead to a 27th sporadic group.

Summary

Why am I discussing this with you today ?

End 2020, I decided to spend some months working on the computer proof-assistant `Lean` and formalize a proof the simplicity theorem.

- Proof-assistants : computer programs that read code whose syntax allows to state both mathematical theorems and their proofs, and whose compilation certifies that the proof is legit. They may, or not, allow some automatization of the process, such as automatic simplifications, up to discovery of (mostly elementary) proofs

Why am I discussing this with you today ?

End 2020, I decided to spend some months working on the computer proof-assistant `Lean` and formalize a proof the simplicity theorem.

- Proof assistants...
- `Lean` is the last born of a long list of such programs, that first appeared in the 1960s. Against it leans `mathlib`, a huge, collaboratory-written, library of mathematical proofs that encompasses many fields of mathematics.

Why am I discussing this with you today ?

End 2020, I decided to spend some months working on the computer proof-assistant `Lean` and formalize a proof the simplicity theorem.

- Proof assistants...
- `Lean` and `mathlib`...
- Only the case $n = 5$ was present in the library. The question posed itself naturally : what proof could/should I try to formalize ?

What do we expect of a proof?

It depends on

- who is “we”,
- what you mean by “proof”,
- and what you mean by “expect”.

I will try to explain this in the context of the simplicity theorem.

What do we expect of a proof ?

We is the mathematician, master or apprentice, but they live in a context :

- (Under)graduate exposition of Galois theory ;
- (Under)graduate exposition of group theory ;
- Research-level exposition of the classification.

Regarding Galois theory, simplicity is not the good objective (non-solvability is much easier, and enough).

About elementary group theory, it makes the theorem a kind of high peak, without any connection with the rest of the discourse, nor accessible consequences.

From a higher-level perspective, it suggests developing the theory of permutation groups, and establishing the simplicity of many groups (notably those appearing in the classification).

What do we expect of a proof ?

Consider a normal subgroup G of $\mathfrak{A}_n$, distinct from 1. Here are three sketches of a proof that $G = \mathfrak{A}_n$.

- Cardinality arguments (for $\mathfrak{A}_5$). If G contains an element g, it contains its conjugacy class, hence the sum of the cardinalities of some conjugacy classes should add up to $\mathrm{Card}(G)$ which divides 60. Look up and conclude.
- (Jordan, essentially) Take an element of $g \in G$, $g \neq 1$, that acts minimally on $\{1, \ldots, n\}$; by (clever ?) manipulations, prove that it is a 3-cycle, and conclude.
- Use a criterion invented by Iwasawa (1941) to prove the simplicity of groups of Lie type. (More about this later).

What do we expect of a proof ?

Consider a normal subgroup G of $\mathfrak{A}_n$, distinct from 1. Here are three sketches of a proof that $G = \mathfrak{A}_n$.

- Cardinality arguments (for $\mathfrak{A}_5$). If G contains an element g, it contains its conjugacy class, hence the sum of the cardinalities of some conjugacy classes should add up to $\mathrm{Card}(G)$ which divides 60. Look up and conclude.
- (Jordan, essentially) Take an element of $g \in G$, $g \neq 1$, that acts minimally on $\{1, \ldots, n\}$; by (clever ?) manipulations, prove that it is a 3-cycle, and conclude.
- Use a criterion invented by Iwasawa (1941) to prove the simplicity of groups of Lie type. (More about this later).

Which one should one prefer ? When ? why ?

What do we expect of a proof ?

Many mathematical/philosophical options :

- A proof is a proof, it proves a theorem, and that's it !
- The shorter a proof, the better...
- A proof should not use theorems that are foreign to the context of its statement.
- A proof can make its statement appear as a corollary, or a particular case, of another, "better" statement.
- A proof can provide some computational content to its statement.

What did I expect of a proof of the simplicity theorem ?

My work on the simplicity theorem has been driven by many diverging forces :

- It is quite difficult to state explicitly to a proof-assistant the informal arguments that we sketch on a blackboard. At first, this also ruled out some of the simplest proofs that rely on case disjunctions.
- Moreover, those proofs have a kind of "magical" character, it is hard to see **why** they work.
- I wanted to provide a proof which is "universal", working for all $n \geqslant 5$ at once and was attracted by the Iwasawa criterion.
- In the end, it appeared that using that criterion connected the proof of the simplicity theorem to more structural results of finite group theory.

Summary

The Iwasawa criterion

Theorem (Iwasawa (1941))

*Let G be a group acting **primitively** on a set X.*

For each $x \in X$, assume given a commutative subgroup A_x of G such that $A_{g \cdot x} = gA_xg^{-1}$ for all $g \in G$ and $x \in X$.

Assume that the subgroups A_x generate G.

Then any normal subgroup N of G which acts nontrivially on X contains the derived subgroup G'.

Used by Iwasawa to prove the simplicity of $\mathrm{PSL}(n, F)$ for any field F (of cardinality at least 4 if $n = 2$).

He indicates in a footnote that his proof applies to symplectic groups as well.

The Iwasawa criterion — comments

- To conclude to simplicity, one needs to show that $G' = G$.
- Primitive actions were defined by Galois ; it means that there is no decomposition of X into "blocks" which are either fixed or permuted by the elements of G.
- An equivalent assumption is that stabilizers G_x of points of X are maximal subgroups of G.
- This assumption is used through a consequence : a normal subgroup of G that acts nontrivially on X acts transitively.

Applying the Iwasawa criterion to the alternating group

One lets $\mathfrak{A}_n$ act on the set X_3 of triples in $\{1, \ldots, n\}$.

For $x = \{a_1, a_2, a_3\} \in X_3$, one sets A_x as the alternating group of x, fixing all other elements.

Then $A_x = \{1; (a_1, a_2, a_3); (a_1, a_3, a_2)\}$ is cyclic of order 3, hence commutative.

The relation $A_{g \cdot x} = g A_x g^{-1}$ is elementary.

The subgroups A_x generate $\mathfrak{A}_n$ (because, as is classical, the 3-cycles generate $\mathfrak{A}_n$).

If $n > 3$, then the action is nontrivial.

If $n \geqslant 5$, the group $\mathfrak{A}_n$ is equal to its derived subgroup.

So **if** the action of $\mathfrak{A}_n$ on X_3 is primitive, then $\mathfrak{A}_n$ is simple.

Applying the Iwasawa criterion to the alternating group

Up to know, we have seen that **if the action of $\mathfrak{A}_n$ on X_3 is primitive, then $\mathfrak{A}_n$ is simple.**

The primitivity of that action looks as a nontrivial result, but it is a classical one.

It amounts to the fact that the subgroup

$$(\mathfrak{S}_3 \times \mathfrak{S}_{n-3}) \cap \mathfrak{A}_n$$

is maximal, which holds for $n > 3$ with the exception $n = 6$.

It is also one of the easy instances in a theorem due to O'Nan and Scott (around 1970) classifying all maximal subgroups of $\mathfrak{A}_n$.

Applying the Iwasawa criterion to the alternating group

However, the papers of O'Nan and Scott give no proof that this subgroup is maximal, they only prove a result of the form "a maximal subgroup belongs to the following list" !

Liebeck, Praeger, Saxl (1987) give the explicit and unambiguous list of the maximal subgroups of $\mathfrak{A}_n$.

However, the case of interest is essentially marked as "well-known".

Sketch : Let G be a subgroup such that $(\mathfrak{S}_3 \times \mathfrak{S}_{n-3}) \cap \mathfrak{A}_n \subsetneq G \subset \mathfrak{A}_n$. To prove that $G = \mathfrak{A}_n$, prove that G acts primitively on $\mathfrak{A}_n$ and apply a theorem of Jordan (1872) : a primitive subgroup of $\mathfrak{S}_n$ that contains a 3-cycle contains $\mathfrak{A}_n$.

Summary

Conclusion

The proof I described is certainly not the simplest and, for many mathematicians, would probably not qualify at relevant.

For me, its interest was 3-fold :

- It relates a basic theorem with on one side the classic concept **primitivity**, and on the other side, the modern perspective of the classification of **maximal subgroups** ;
- It offers a unifying perspective on the proofs of simplicity, as its scheme seems to be applicable to similar theorems ;
- Writing it led me to learn unsuspected mathematics, as well as to reflect (at least to try to) on the idea of a proof.