Simplicity — Group actions and proof formalization

Antoine Chambert-Loir (*Université Paris Cité*)

Mini symposium on the occasion of the
Inaugural lecture of Assia Mahboubi
VU Amsterdam
26 april 2023

Abstract

The theorem that the alternating group in at least 5 letters is a simple group is a cornerstone of many group theory courses, sometimes in connection with Abel's theorem that the general equation of degree at least 5 is not solvable by radicals.

The first part of this talk is an introduction to the field of proof assistants.

In a second part, I describe the mathematics underlying my formalization of the above mentioned theorem that relies on a classic criterion of Iwasawa.

More details are given in my paper "Formalizing the proof of an intermediate-level algebra theorem – An experiment", `https://arxiv.org/abs/2303.12404`.

Summary

Formalism

Simplicity

Primitivity

Maximality

Mathematical formulas and formal mathematics

End of 19th c., beginning of 20th c. :

- Need for more precise definitions (Dedekind, Heine, Cantor, Zermelo...)
- Several enterprises of formal, purely symbolic, writings of mathematics, starting from first axioms.

Giuseppe Peano

G. Peano (1890), *Introduction au tome II du « Formulaire de mathématiques »*

Gottfried Wilhelm Leibniz, pendant toute sa vie (1646-1716) s'est occupé d'« une manière de Spécieuse Générale, où toutes les vérités de raison seroient réduites à une façon de calcul. Ce pourit être en même tems une manière de Langue ou d'Écriture universelle, mais infiniment différente de toutes celles qu'on a projetées jusqu'ici ; car les caractères, et les paroles mêmes, y dirigeroient la Raison ; et les erreurs (excepté celles de fait) n'y seroient que des erreurs de calcul. Il seroit très difficile de former ou d'invonter cette langue ou caractéristique ; mais très aisé de l'apprendre sns aucuns dictionnaires » (*Opera philosophica*, a. 1840, p. 701).

Giuseppe Peano

G. Peano (1890), *Introduction au tome II du « Formulaire de mathématiques »*

Gottfried Wilhelm Leibniz, during all his life (1646-1716) handled about “a sort of Universal Characteristic, in which all truths of reason would be reduced to some sort of calculus. It could be a kind of Language or universal Script, but infinitely different from all of those which have been imagined until now; because the characters, and even the words, would conduct Reason; and the mistakes (but for mistakes of facts) would only be calculation mistakes. It would be very difficult to form or to invent this language or characterisic, but very easy to learn it without any dictionary” (*Opera philosophica*, a. 1840, p. 701).

Alfred N. Whitehead & Bertrand Russell

A. N. Whitehead & B. Russell (1927), *Principia mathematica*

We have found it necessary to give very full proofs, because otherwise it is scarcely possible to see what hypotheses are really required, or whether our results follow from our explicit premisses. (It must be remembered that we are not affirming merely that such and such propositions are true, but also that the axioms stated by us are sufficient to prove them.)

N. Bourbaki

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Introduction)

(...) l'analyse du mécanisme des démonstrations dans des textes mathématiques bien choisis a permis d'en dégager la structure, du double point de vue du vocabulaire et de la syntaxe. On arrive ainsi à la conclusion qu'un texte mathématique suffisamment explicite pourrait être exprimé dans une langue conventionnelle ne comportant qu'un petit nombre de « mots » invariables assemblés suivant une syntaxe qui consisterait en un petit nombre de règles inviolables : un tel texte est dit *formalisé*.

N. Bourbaki

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Introduction)

By analysis of the mechanism of proof in suitably chosen mathematical texts, it has been possible to discern the structure underlying both vocabulary and syntax. This analysis has led to the conclusion that a sufficiently explicit mathematical text could be expressed in a conventional language containing only a small number of fixed “words”, assembled according to a syntax consisting of a small number of unbreakable rules : such a text is said to be *formalized*.

N. Bourbaki, again

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Introduction)

Si la mathématique formalisée était aussi simple que le jeu d'échecs, une fois décrit le langage formalisé que nous avons choisi, il n'y aurait plus qu'à rédiger nos démonstrations dans ce langage, comme l'auteur d'un traité d'échecs écrit dans sa notation les parties qu'il se propose d'enseigner, en les accompagnant au besoin de commentaires. Mais les choses sont loin d'être aussi faciles, et point n'est besoin d'une longue pratique pour s'apercevoir qu'un tel projet est absolument irréalisable ; la moindre démonstration du début de la *Théorie des Ensembles* exigerait déjà des centaines de signes pour être complètement formalisée.

N. Bourbaki, again

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Introduction)

If formalized mathematics were as simple as the game of chess, then once our chosen formalized language had been described there would remain only the task of writing out our proofs in this language, just as the author of a chess manual writes down in his notation the games he proposes to teach, accompanied by commentaries as necessary. But the matter is far from being as simple as that, and no great experience is necessary to perceive that such a project is absolutely unrealizable : the tiniest proof at the beginning of the Theory of Sets would already require several hundreds of signs for its complete formalization.

N. Bourbaki, yet again

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Chapitre III)

Une estimation grossière montre que le terme *désigné* [par “1”] est un assemblage de plusieurs dizaines de milliers de signes (chacun de ces signes étant l’un des signes τ, $\square$, $\vee$, $\neg$, $=$, $\in$).

N. Bourbaki, yet again

N. Bourbaki (1935), Éléments de mathématique, *Théorie des ensembles* (Chapitre III)

As a rough estimate, the term so *denoted* [by “1”] is an assembly of several tens of thousands ofsigns (each of which is one of τ, $\square$, $\vee$, $\neg$, $=$, $\in$, $\supset$).

A. R. D. Mathias

A. R. D. Mathias (2002), “A term of length 4 523 659 424 929”. *Synthese*, **133**, 75-86.

Bourbaki suggest that their definition of the number 1 runs to some tens of thousand of symbols. We show that that is a considerable under-estimate, the true number of symbols being that in the title not counting 1 179 618 517 981 links between symbols that are needed to disambiguate the whole expression.

Proof assistants

The rise of computers since the 1950s led to seek to mechanize these verifications. Several softwares were built, notably :

- N.G. De Bruijn, `Automath` (1967)
- A. Trybulec, `Mizar` (1973)
- G. Huet et al., `Coq` (1989)
- C. Coquand, `Agda` (1999)
- L. de Mourra, `Lean` (2013)...

Each of them corresponds to (techno)logical decisions. For example, `Mizar` is built on set theory, `Coq` and `Lean` on dependent type theory, and `Agda` on homotopy type theory.

“Was sind und sollen die Beweisassistenten ?”

Proof assistants are kind of program compilers that “read” theorem statements accompanied by purported proofs, written in an adequate language, and guarantee that these proofs reach indeed their goals.

With varying ability, they also can do themselves simplifications, up to devising small chunks of proofs, roughly at the level of a bachelor exercise.

Proof assistants : landmarks

- G. Gonthier et al. (2008), the 4-color theorem of Appell and Haken
- G. Gonthier et al. (2013), the Feit–Thompson theorem
- T. Hales (2017), the Kepler conjecture (proved by him)
- J. Commelin et al. (2022), a theorem of Scholze in the commutative algebra of condensed mathematics (“Large tensor experiment”)
- P. Massot et al. (2022), Gromov’s h-principle and sphere eversion

Proof assistants : a tool for teaching ?

For some years, colleagues teaching in math or computer science have been using these proof assistants as a tool to proof teaching, at the bachelor level.

D. J. Velleman, *How to prove it : A structured approach*, Cambridge Univ. Press

How to prove it with Lean,
`https://djvelleman.github.io/HTPIwL/`

Proof assistants : an everyday tool for mathematicians ?

Could we imagine that in a near future, our theorems would be directly implemented in such tools ?

Interest :

- Guarantees that proofs are correct ;
- Switches the communication task towards understanding

Difficulties :

- Needs a sort of “mathematical Babel library”
- Software obsolescence
- Bridges between various softwares

Mathlib

The mathematical library *mathlib* is a companion to the software `lean`, more than a million code lines covering a large part of the mathematical spectrum :

- measure theory, ergodic theory
- general algebra, field theory
- complex analysis
- functional analysis
- differential manifolds...

To me, the existence of *mathlib* was an important motivation to participate the `lean` project.

Summary

Formalism

Simplicity

Primitivity

Maximality

Simplicity of the alternating group

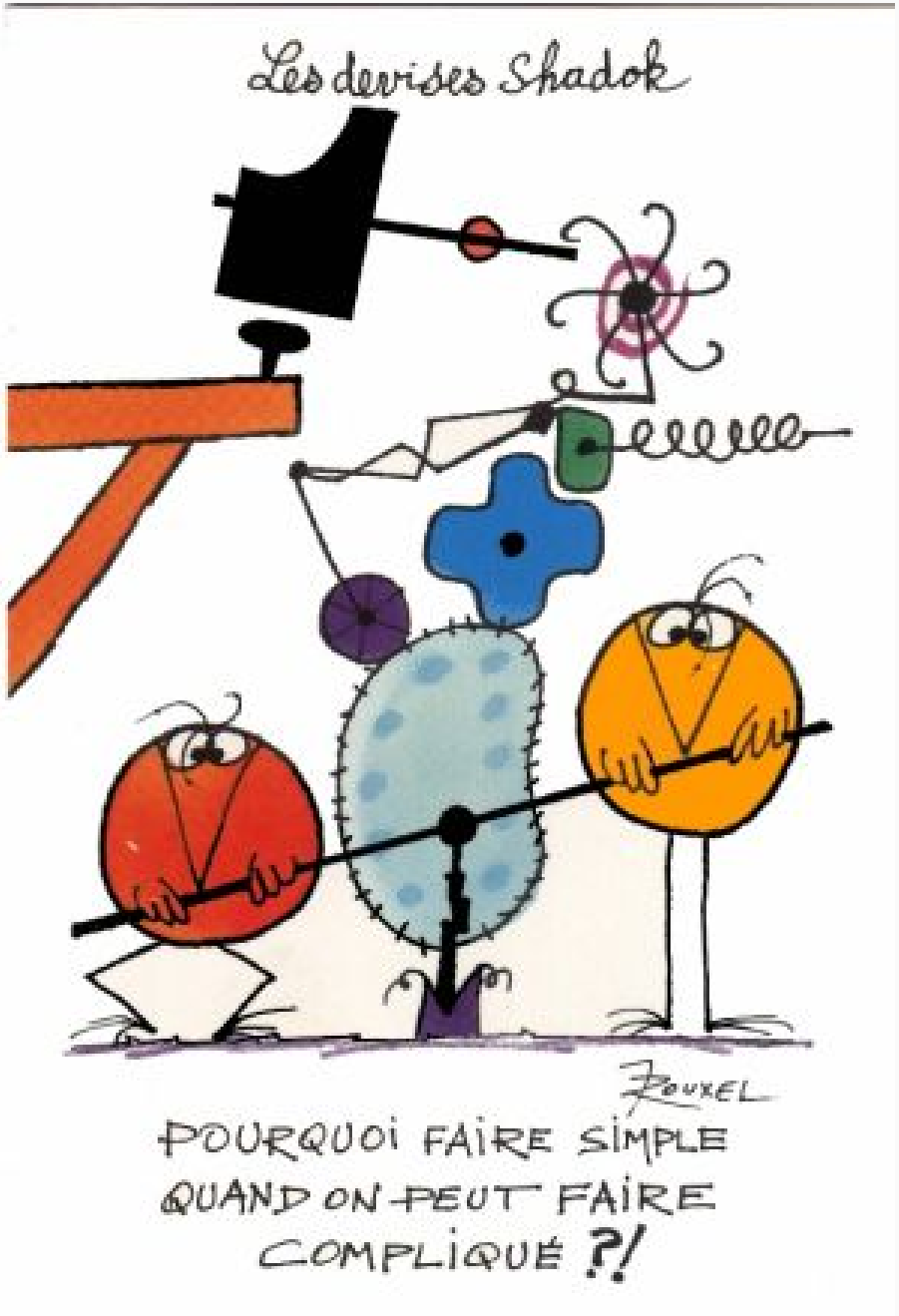
Theorem

For $n \geqslant 5$, the alternating group $\mathfrak{A}_n$ is simple : its only normal subgroups are $\{e\}$ and itself.

Those groups are one of the bricks of the classification of finite simple groups, the other ones being

- cyclic groups of prime order,
- families of groups defined by geometry, such as $\mathrm{PSL}(n, F)$ if F is a finite field of cardinality $\geqslant 4$,
- 26 “sporadic” groups defined by combinatorial geometries.

Pourquoi faire simple quand on peut faire compliqué ?



Pourquoi faire simple quand on peut faire compliqué ?

The simplicity theorem can be — and is often — explained in an undergraduate course. All standard proofs are slightly ad hoc, and often require computations which are typically avoided at the blackboard, and not so easy to communicate in detail, either to a student or to a computer.

I wished to prove that theorem in a more geometric manner using the general simplicity criterion introduced by Iwasawa (1941) to prove the simplicity of geometric groups.

This criterion is also used to prove the simplicity of sporadic groups, such as the Mathieu groups.

Iwasawa's criterion

Proposition (Iwasawa, 1941)

Let G be a group acting on a set X. One assumes that the action is 2-transitive and that, for every $x \in X$, one is given a subgroup A_x of G such that

- *For $g \in G$ and $x \in X$, one has $A_{g \cdot x} = gA_xg^{-1}$;*
- *The groups A_x are commutative and their union generates G.*

Then every normal subgroup of G that acts nontrivially on X contains the derived subgroup G' of G.

Derived subgroup

Reminder : it is the subgroup generated by commutators $g^{-1}h^{-1}gh$.

(Smallest kernel of a morphism to a commutative group.)

Examples :

- $\mathfrak{A}_n' = \mathfrak{A}_n$ for $n \geqslant 5$. This implies that $\mathfrak{A}_n$ is not solvable (hence applications to Galois theory) but is much easier than simplicity.
- $\mathrm{SL}(n, F)' = \mathrm{SL}(n, F)$ for $n \geqslant 3$ or $\mathrm{Card}(F) > 4$.

“Simplicity” of $\mathrm{SL}(n, F)$

Let V be a vector space of finite dimension $\geqslant 2$ on a field F. For $\dim(V) \geqslant 3$ or $\mathrm{Card}(F) \geqslant 4$, the group $\mathrm{PSL}(V)$ is simple.

We let $\mathrm{SL}(V)$ act on the projective space $\mathbf{P}(V)$, the space of lines in V.

The action is 2-transitive.

For a line $D \subseteq V$, let A_D be the set of all transvections u of the form $x \mapsto x + \varphi(x)e$, where $\varphi \in V^*$, $e \in D$ and $D \subseteq \ker(\varphi)$. It is a commutative subgroup of $\mathrm{SL}(V)$.

One has $A_{g \cdot D} = g A_D g^{-1}$. These groups generate $\mathrm{SL}(V)$.

Iwasawa : Every normal subgroup N of $\mathrm{SL}(V)$ that acts nontrivially on $\mathbf{P}(V)$ contains the derived subgroup $\mathrm{SL}(V)'$.

Condition : N is not contained in the center of $\mathrm{SL}(V)$.

Simplicity of $\mathfrak{A}_5$

We apply Iwasawa's criterion to the action of $\mathfrak{A}_5$ on $X = \{1, 2, 3, 4, 5\}$.

For $x \in X$, define A_x as the subgroup of double transpositions that fix x : it is a Klein group.

- This action is 2-transitive.
- Conjugation relation $A_{g \cdot x} = g A_x g^{-1}$
- These groups generate $\mathfrak{A}_5$.

Conclusion : **Every nontrivial normal subgroup of $\mathfrak{A}_5$ contains the derived subgroup, hence is equal to $\mathfrak{A}_5$.**

Simplicity of $\mathfrak{A}_n$

We will apply a variant of Iwasawa's criterion to the action of $\mathfrak{A}_n$ on the set of k-element subsets of $X = \{1, \ldots, n\}$ for $k = 3$ or $k = 4$.

If S is such a subset, define A_S as

- the alternating group $\mathfrak{A}_S$ of this subset for $k = 3$ (isomorphic to $\mathbf{Z}/3\mathbf{Z}$),
- the group of double transpositions supported by this subset for $k = 4$ (isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$).

One has $A_{g.S} = gA_Sg^{-1}$, and these groups generate $\mathfrak{A}_n$.

Simplicity of $\mathfrak{A}_n$

We will apply a variant of Iwasawa's criterion to the action of $\mathfrak{A}_n$ on the set of k-element subsets of $X = \{1, \ldots, n\}$ for $k = 3$ or $k = 4$.

If S is such a subset, define A_S as

- the alternating group $\mathfrak{A}_S$ of this subset for $k = 3$ (isomorphic to $\mathbf{Z}/3\mathbf{Z}$),
- the group of double transpositions supported by this subset for $k = 4$ (isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$).

One has $A_{g.S} = gA_Sg^{-1}$, and these groups generate $\mathfrak{A}_n$.

Problem : the action is not 2-transitive.

Summary

Formalism

Simplicity

Primitivity

Maximality

Primitive actions

Let a group G act on a set X. A **block** of X is a subset $B \subseteq X$ such that for every $g \in G$, either $B = g \cdot B$, or $B \cap g \cdot B = \emptyset$.

$B = \emptyset$, singletons, $B = X$ are blocks, called *trivial*.

Definition

*The action of G on X is **primitive** if the only blocks are trivial.*

Variant : the only equivalence relations on X which are compatible with the action of G are trivial (coarse or discrete).

Introduced by Galois in his letter to Auguste Chevalier : then X is the set of roots of a polynomial, acted on by the Galois group G.

Transitivity and primitivity

An orbit is a block, hence **a primitive action is transitive.**

Transitivity and primitivity

An orbit is a block, hence **a primitive action is transitive.**

A 2-transitive action is primitive.

Let B be a nontrivial block.
Let $x \neq y \in B$, and let $z \in X \setminus B$.
By 2-transitivity, there is $g \in G$ such that $g \cdot x = x$ et $g \cdot y = z$.
Then $x \in B \cap g \cdot B$, hence $B = g \cdot B$.
Since $y \in B$ and $z = g \cdot y$, we get $z \in B$; contradiction.

The Iwasawa criterion for primitive actions

Let N be a normal subgroup of G that acts nontrivially on X.

- **N acts transitively on X :** since N is normal, the orbit of N is a block.
- **For any $x, y \in X$, we have $A_y \leqslant \langle N, A_x \rangle$.** Write $y = n \cdot x$, for $n \in N$. Then $A_y = n \cdot A_x \cdot n^{-1} \leqslant \langle N, A_x \rangle$.
- Fix $x \in X$. Since the A_y generate G, we have $G = \langle N, A_x \rangle$.
- The morphism $A_x \to G \to G/N$ is surjective, hence G/N is abelian, hence N contains the derived subgroup of G.

Primitive actions : geometry

The action of $\mathrm{SO}(3, \mathbf{R})$ on $\mathrm{P}_3(\mathbf{R})$ is primitive.

- *It is transitive :* if u, v are unit vectors, there is $g \in \mathrm{SO}(3, \mathbf{R})$ such that $g \cdot u = v$.
- *It is not 2-transitive :* rotations preserve angles
- *It is primitive :* if a block contains (the lines through) the north pole and another point, it contains the whole parallel, then the sphere.

This implies that $\mathrm{SO}(3, \mathbf{R})$ is simple.

Primitive actions : geometry

The action of $\mathrm{SO}(3, \mathbf{R})$ on $\mathrm{P}_3(\mathbf{R})$ is primitive.

- *It is transitive :* if u, v are unit vectors, there is $g \in \mathrm{SO}(3, \mathbf{R})$ such that $g \cdot u = v$.
- *It is not 2-transitive :* rotations preserve angles
- *It is primitive :* if a block contains (the lines through) the north pole and another point, it contains the whole parallel, then the sphere.

This implies that $\mathrm{SO}(3, \mathbf{R})$ is simple.

General case — For "non compact" orthogonal groups, Tamagawa (1958)

Primitive actions : combinatorics

For $n \geqslant 3$ and $k \neq 0, n/2, n$, the action of $\mathfrak{A}_n$ on the k-element subsets of $\{1, \ldots, n\}$ is primitive.

Subtle (see later).

- *It is transitive :*
- *It is not 2-transitive :* because $\mathrm{Card}(g \cdot A \cap g \cdot B) = \mathrm{Card}(A \cap B)$.

Simplicity of $\mathfrak{A}_n$

We get a slightly complicated, geometric, proof of the simplicity of $\mathfrak{A}_n$, for $n \geqslant 5$:

- If $n \neq 8$, take $k = 4$, and A_S to be the Klein group with support in S.
- If $n \neq 6$, take $k = 3$, and A_S to be the alternating group with support in S.

Summary

Formalism

Simplicity

Primitivity

Maximality

Primitivity and maximality

Proposition

Let G be a group acting transitively and nontrivially on a set X.

The action of G on X is primitive

$\Leftrightarrow$ *For every $x \in X$, the fixator G_x of x is a maximal subgroup of G.*

More generally, the maps

$$B \mapsto G_B, \qquad H \mapsto H \cdot x$$

are increasing bijections between the set of block of X containing x and the set of subgroups of G containing G_x.

Maximal subgroups

In view of Iwasawa's criterion, this justifies to study systematically the maximal subgroups of a given group G.

For finite simple groups, this study appears as a step in the description of the classification of finite simple groups. They are made explicit :

- by a theorem of O'Nan–Scott (1980–81) for the symmetric/alternating groups ;
- by a theorem of Aschbacher (1984) for classical groups on a finite field.

The O'Nan–Scott theorem

Let G be a maximal subgroup of $\mathfrak{A}_n$. Then G is the trace on $\mathfrak{A}_n$ of one of the following groups :

- $G = \mathfrak{S}_k \times \mathfrak{S}_{n-k}$ for $0 < k < n - k < n$ (intransitive case)
- $G = \mathfrak{S}_k \wr \mathfrak{S}_m$, where $n = mk$ and $m, k > 1$ (imprimitive case)
- $n = p^k$ and G is the affine group of $\mathbf{F}_{p^k}$

and three other cases.

Note these subgroups appear as stabilizers of natural structures — in the first two cases, a partition.

The converse : Liebeck, Praeger, Saxl (1987)

All of the subgroups in the list of O'Nan–Scott are maximal, up to some exceptions.

In particular, if $1 \leqslant k < n/2$ (and $n \geqslant 5$), then the stabilizer in $\mathfrak{A}_n$ of a k-element subset of $\{1, \ldots, n\}$ is a maximal subgroup of $\mathfrak{A}_n$.

In other words, the action of $\mathfrak{A}_n$ on the k-element subsets of $\{1, \ldots, n\}$ is primitive.

This is exactly what was needed to conclude our not-so-simple proof of the simplicity of $\mathfrak{A}_n$.

Proof of the primitivity result

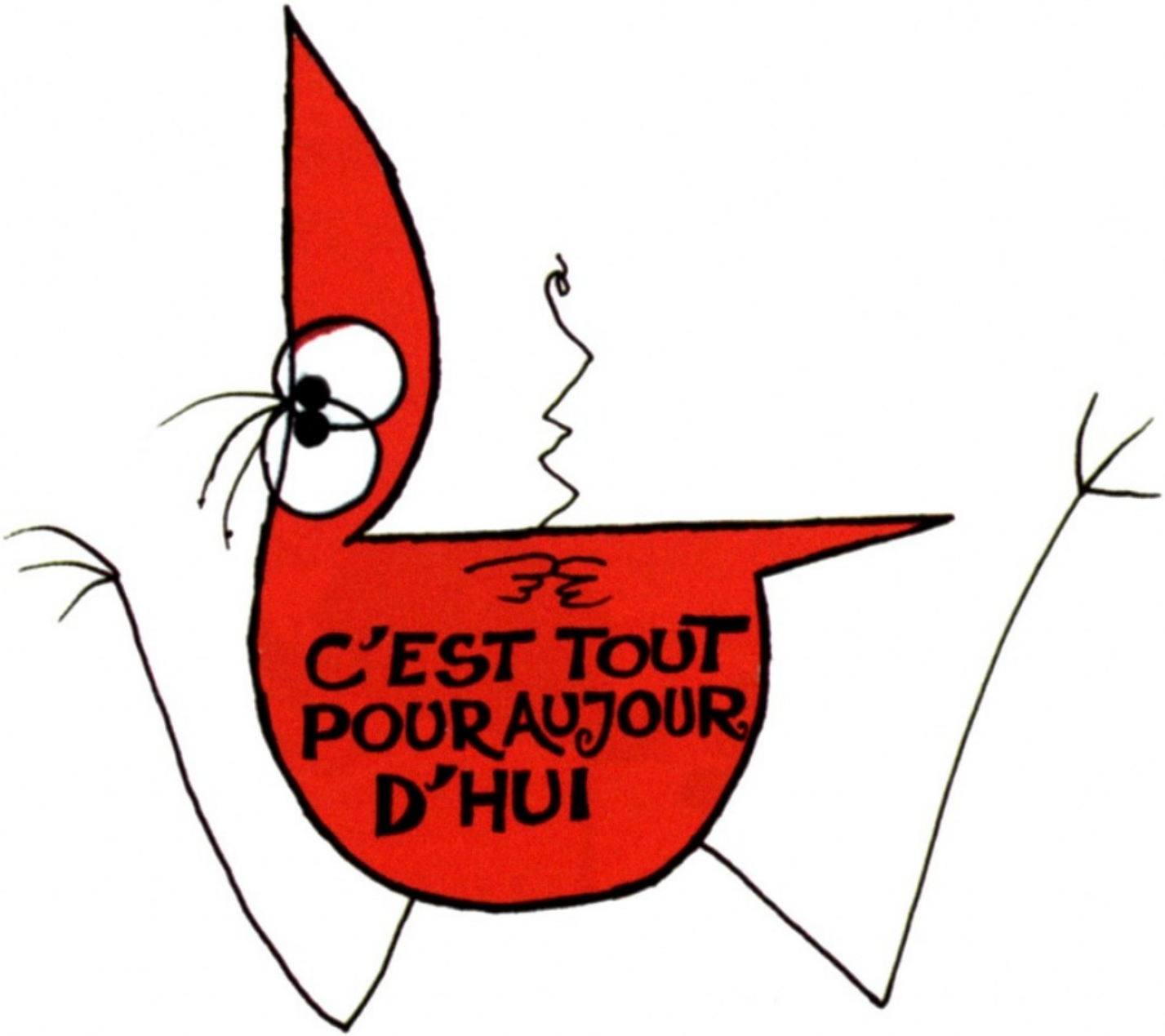
Proposition

Let $k, n \in \mathbf{N}$ be such that $n \geqslant 5$ and $1 \leqslant k < n - k$. Then the subgroup $G = (\mathfrak{S}_k \times \mathfrak{S}_{n-k}) \cap \mathfrak{A}_n$ of $\mathfrak{A}_n$ is maximal.

Assume $k = 1$. Then G is the fixator of $\{1\}$. For $n \geqslant 3$, the action of $\mathfrak{A}_n$ on $\{1, \ldots, n\}$ is 2-transitive, hence primitive, hence G is maximal.

Assume $k \geqslant 2$. Let H be a group such that $G < H \leqslant \mathfrak{A}_n$; we want to prove that $H = \mathfrak{A}_n$. This is done in two steps :

- We prove that H acts primitively on $\{1, \ldots, n\}$; here that requires $k \neq n - k$.
- We conclude by a theorem of Jordan (1870) : **A primitive subgroup of $\mathfrak{S}_n$ that contains a 3-cycle contains $\mathfrak{A}_n$.**


C'EST TOUT
POUR AUJOUR
D'HUI