Simplicité des groupes
Une expérience incomplète de formalisation

Antoine Chambert-Loir (*Université Paris Cité*, IMJ-PRG)

Séminaire Formath, 13 novembre 2023

Résumé

La notion de groupe simple apparaît dans les travaux de Galois en relation avec la résolubilité par radicaux des équations polynomiales.

Je présenterai mon travail sur la formalisation en `Lean` de la simplicité du groupe alterné sur au moins 5 lettres qui repose sur un critère d'Iwasawa.

Ce théorème, souvent attribué à Galois lui-même, possède de nombreuses preuves, certaines assez courtes, et celle que j'ai choisie est en fin de compte assez longue.

Je tenterai de justifier pourquoi son schéma, les concepts qu'elle met en œuvre et les ramifications qu'elle offre la rendent, à mon sens, appropriée pour figurer dans une librairie de mathématiques formelles.

"Formalizing the proof of an intermediate-level algebra theorem – An experiment", `https://arxiv.org/abs/2303.12404`.

Sommaire

Simplicité du groupe alterné

Théorème

Soit n un entier, $n \geqslant 5$. Le groupe alterné $\mathfrak{A}_n$ est un groupe simple.

```
/-- If ‘X‘ has at least 5 elements, then ‘alternatingGroup X‘ is simple.
    -/
theorem alternatingGroup.isSimpleGroup {X : Type*} [DecidableEq X]
    [Fintype X]
    (hX : 5 ⩽ Fintype.card X) :
    IsSimpleGroup (alternatingGroup X) := by
  sorry
```

Listing 1 – Simplicité du groupe alterné : code Lean

Simplicité du groupe alterné

Théorème

Soit n un entier, $n \geqslant 5$. Le groupe alterné $\mathfrak{A}_n$ est un groupe simple.

Rappel de définitions :

- Le **groupe alterné** $\mathfrak{A}_n$ est le groupe des permutations $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ qui sont de signature $+1$ — de manière équivalente, produits d'un nombre **pair** de transpositions (i, j).
- Un groupe est **simple** s'il n'est pas trivial et si ses seuls sous-groupes distingués sont $\{1\}$ et lui-même. Moralement : ne peut pas être construit à partir de deux groupes plus simples.

Sous-groupes distingués et groupes simples

Autre rappel :

- Un sous-groupe H d'un groupe G est **distingué** (english : "normal") si $ghg^{-1} \in H$ pour tout $g \in G$ et tout $h \in H$ — de manière équivalente, il y a une relation d'équivalence sur G qui est compatible à la loi de groupe et telle que H est la classe de 1.

Sous-groupes distingués « évidents » d'un groupe G :

- Le sous-groupe trivial $\{1\}$, le groupe G lui-même ;
- Si G est commutatif, tous ses sous-groupes sont distingués ;
- Le centre $Z(G)$ de G ;
- Le sous-groupe dérivé G' de G, engendré par les commutateurs $ghg^{-1}h^{-1}$.

Théorie de Galois des équations polynomiales (1830)

La notion de sous-groupe distingué est due à Galois (1830) en relation avec la question de la résolubilité par radicaux des équations polynomiales, résolue par Abel (1824) après une solution partielle de Ruffini (1799/1813).

Galois démontre qu'une équation polynomiale est résoluble par radicaux si et seulement si son groupe de Galois est « résoluble ».

Une conséquence du résultat de simplicité est qu'une équation de degré $n \geqslant 5$ générale (dont le groupe est $\mathfrak{S}_n$) n'est pas résoluble par radicaux, mais cela est plus facilement démontré directement.

La classification des groupes finis simples (1950-2010)

Sauf erreur, on connaît la liste des groupes finis simples. Il y en a 4 sortes :

- Groupes finis cycliques de cardinal premier $(\mathrm{Z}/p\mathrm{Z})$;
- Les groupes alternés $\mathfrak{A}_n$, pour $n \geqslant 5$;
- Des groupes d'origine géométrique, définis via l'algèbre linéaire, tels que $\mathrm{PSL}(n, F)$, pour $n \geqslant 2$ et F un corps fini (de cardinal $\geqslant 4$ si $n = 2$) ;
- Une liste de 26 groupes « sporadiques », de définition combinatoire, débutant avec les groupes de Mathieu M_{11} et M_{12} (1861), jusqu'au groupe de Janko J_4 (1974) et au **Monstre** de Griess-Fischer dont l'existence et l'unicité a été établie vers 1980.

La classification des groupes finis simples (1950-2010)

La preuve de cette classification est démesurément longe et difficile, plus de 100 auteurs, des centaines d'articles, des dixaines de milliers de pages ; une révision (1994) et une mise à jour récente qui résout une erreur découverte en 1979.

Elle a des applications (parfois immédiates) à des questions de théorie des groupes, lorsqu'elles se réduisent à des propriétés des groupes finis simples.

Il est probable qu'elle contient des erreurs ; certains mathématiciens préfèrent ne pas l'utiliser. Cependant, il est peu probable que ces erreurs conduiraient à un 27^{e} groupe sporadique, encore moins à une nouvelle liste.

Sommaire

Pourquoi je suis en train de vous raconter çà...

À la fin 2020, je me suis embarqué dans l'apprentissage de l'assistant de preuve `Lean` et j'ai alors décidé de formaliser la démonstration du théorème de simplicité du groupe alterné.

Pourquoi ?

Pourquoi je suis en train de vous raconter çà...

À la fin 2020, je me suis embarqué dans l'apprentissage de l'assistant de preuve `Lean` et j'ai alors décidé de formaliser la démonstration du théorème de simplicité du groupe alterné.

Pourquoi ?

- Pourquoi `Lean` : Raisons « médiatiques » ; Bibliothèque de mathématiques `mathlib` : déjà assez développée, généraliste, « ouverture »...
- Pourquoi ce théorème : n'était pas formalisé (sauf pour $n = 5$), et est d'un niveau intermédiaire entre « généralités » et résultats très avancés que `mathlib` aime mettre en avant.

Démonstrations du théorème de simplicité

Soit G un sous-groupe distingué de $\mathfrak{A}_n$ ($n \geqslant 5$), distinct de $\{1\}$. Comment prouver que $G = \mathfrak{A}_n$?

- Arguments de comptage (pour $\mathfrak{A}_5$). Par exemple : si G contient un élément g, il contient sa classe de conjugaison, donc la somme des cardinaux de certains classes de conjugaison égale le cardinal de G, qui divise 60. Regarder et conclure.
- Jordan (1870, essentiellement) : considérer un élément $g \in G$ distinct de 1 qui agit minimalement sur $\{1, \ldots, n\}$; par des manipulations (astucieuses ?), démontrer que c'est un 3-cycle et conclure.
- Utiliser un critère d'Iwasawa (1941) inventé pour démontrer la simplicité de groupes d'origine géométrique.

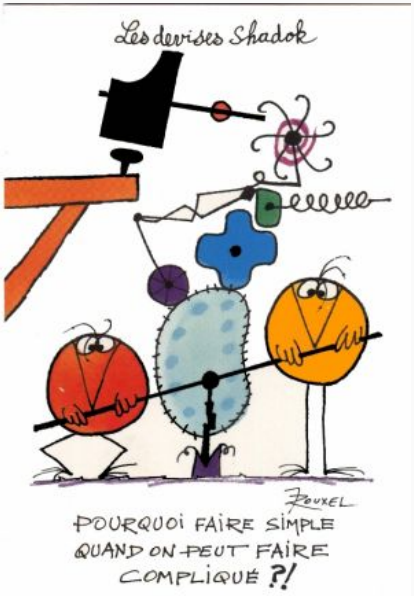
Démonstrations du théorème de simplicité

Soit G un sous-groupe distingué de $\mathfrak{A}_n$ ($n \geqslant 5$), distinct de $\{1\}$. Comment prouver que $G = \mathfrak{A}_n$?

- Arguments de comptage (pour $\mathfrak{A}_5$). Par exemple : si G contient un élément g, il contient sa classe de conjugaison, donc la somme des cardinaux de certains classes de conjugaison égale le cardinal de G, qui divise 60. Regarder et conclure.
- Jordan (1870, essentiellement) : considérer un élément $g \in G$ distinct de 1 qui agit minimalement sur $\{1, \ldots, n\}$; par des manipulations (astucieuses ?), démontrer que c'est un 3-cycle et conclure.
- Utiliser un critère d'Iwasawa (1941) inventé pour démontrer la simplicité de groupes d'origine géométrique.

Laquelle choisir ?

Pourquoi faire simple...



Pourquoi faire simple...

La démonstration que `mathlib` connaît pour $\mathfrak{A}_5$ est celle par comptage ; on peut compléter par une preuve par récurrence sur n. (Je ne l'ai pas fait, peut-être à tort ; cela vaudrait probablement la peine de dégager un énoncé général et raisonnable.)

La démonstration de Jordan prend quelques lignes dans les manuels d'algèbre, avec pas mal de points de suspension et d'agitation des mains. J'avais peu confiance que ce fût facilement explicable à l'ordinateur ; en fait, ça l'est.

Le critère d'Iwasawa a l'intérêt d'être réutilisable pour prouver d'autres théorèmes de simplicité, de façon plus uniforme (groupes géométriques, groupes de Mathieu). Il met aussi en évidence un lien avec la structure des sous-groupes maximaux d'un groupe donné.

Le critère d'Iwasawa

Proposition (Iwasawa, 1941)

Soit G un groupe opérant sur un ensemble X. On suppose que l'action est 2-transitive et que pour tout $x \in X$, on dispose d'un sous-groupe A_x de G tels que

- *Pour $g \in G$ et $x \in X$, on a $A_{g \cdot x} = gA_x g^{-1}$;*
- *Les groupes A_x sont commutatifs et leur réunion engendrent G.*

Alors tout sous-groupe distingué de G qui agit non trivialement sur X contient le groupe dérivé G' de G.

Le critère d'Iwasawa

Proposition (Iwasawa, 1941)

Soit G un groupe opérant sur un ensemble X. On suppose que l'action est 2-transitive et que pour tout $x \in X$, on dispose d'un sous-groupe A_x de G tels que

- *Pour $g \in G$ et $x \in X$, on a $A_{g \cdot x} = gA_x g^{-1}$;*
- *Les groupes A_x sont commutatifs et leur réunion engendrent G.*

Alors tout sous-groupe distingué de G qui agit non trivialement sur X contient le groupe dérivé G' de G.

Double transitivité : pour $x \neq x'$ et $y \neq y'$, il existe $g \in G$ tel que $g \cdot x = x'$ et $g \cdot y = y'$.

L'hypothèse interviant sous sa conséquence (plus faible) : tout sous-groupe distingué qui agit non trivialement agit transitivement.

Le critère d'Iwasawa

```
variables {G X : Type*} [Group G ][MulAction G X]
/-- The structure underlying the Iwasawa criterion -/
structure IwasawaStructure where
  T : X → Subgroup G
  is_comm : ∀ x : X, (T x).IsCommutative
  is_conj : ∀ g : G, ∀ x : X, T (g · x) = MulAut.conj g · T x
  is_generator : iSup T = ⊤
/-- The Iwasawa criterion -/
theorem Iwasawa.commutator_le
    (is_qprim : IsQuasipreprimitive G X)
    (IwaS : IwasawaStructure G X)
    {N : Subgroup G} (nN : N.Normal)
    (hNX : MulAction.fixedPoints N X ≠ ⊤) :
    commutator G ⩽ N := by sorry
```

Listing 2 – Critère d'Iwasawa, Lean

Le critère d'Iwasawa

```
/-- The Iwasawa criterion: simplicity -/
theorem Iwasawa.isSimpleGroup
    (is_nontrivial : Nontrivial G) (is_perfect : commutator G = ⊤)
    (is_qprim : IsQuasipreprimitive G X) (is_faithful : FaithfulSMul G X)
    (IwaS : IwasawaStructure G X) : IsSimpleGroup G := by
```

Listing 3 – Iwasawa Criterion : application to simplicity, in Lean

Groupe dérivé

Rappel : c'est le sous-groupe engendré par les commutateurs.

(Plus petit noyau d'un morphisme vers un groupe commutatif.)

Exemples :

- $\mathfrak{A}_n' = \mathfrak{A}_n$ si $n \geqslant 5$, et c'est bien plus facile que la simplicité (lié à la non-résolubilité de $\mathfrak{A}_n$).
- $\mathrm{SL}(n, F)' = \mathrm{SL}(n, F)$ (si $n = 2$, $\mathrm{Card}(F) \geqslant 4$).

“Simplicité” de $\mathrm{SL}(n, F)$

Soit V un espace vectoriel de dimension finie $\geqslant 2$ sur un corps F. On fait agir $\mathrm{SL}(V)$ sur l'espace des droites de V, qui est l'espace projectif $\mathrm{P}(V)$. L'action est 2-transitive.

Pour une droite $D \subseteq V$, on note A_D l'ensemble des transvections u de la forme $x \mapsto x + \varphi(x)e$, où $e \in D$ et $D \subseteq \ker(\varphi)$. C'est un sous-groupe commutatif de $\mathrm{SL}(V)$.

On a $A_{g \cdot D} = gA_Dg^{-1}$.

Ces groupes engendrent $\mathrm{SL}(V)$.

Tout sous-groupe distingué N de $\mathrm{SL}(V)$ qui agit non trivialement sur $\mathrm{P}(V)$ contient donc le sous-groupe des commutateurs de $\mathrm{SL}(V)$. La condition est que N ne soit pas contenu dans le centre de $\mathrm{SL}(V)$.

Si $\dim(V) \geqslant 3$ *ou* $\mathrm{Card}(F) \geqslant 4$, *alors* $\mathrm{PSL}(V)$ *est simple.*

Preuve du critère d'Iwasawa

Soit N un sous-groupe distingué de G qui opère non trivialement sur X.

- Soit $x \in X$. On va prouver $G = \langle N, A_x \rangle$.
- Soit $y \in X$; il existe $n \in N$ tel que $n \cdot x = y$ (c'est l'hypothèse sur l'action de G sur X !) et $A_y = nA_x n^{-1} \subset \langle N, A_x \rangle$.
- Comme G est engendré par les A_y, on a $G \subset \langle N, A_x \rangle$, d'où l'égalité.
- L'homomorphisme composé $A_x \to G \to G/N$ est donc surjectif.
- Donc G/N est commutatif et N contient G'.

Simplicité de $\mathfrak{A}_5$

On applique le critère d'Iwasawa à l'action de $\mathfrak{A}_5$ sur $X = \{1, 2, 3, 4, 5\}$.

Pour $x \in X$, on définit A_x comme le groupe des double-transpositions qui fixent x : c'est un groupe de Klein.

- Cette action est 2-transitive.
- Relation de conjugaison $A_{g \cdot x} = g A_x g^{-1}$
- Ils engendrent $\mathfrak{A}_5$.

Conclusion : tout sous-groupe distingué non trivial de $\mathfrak{A}_5$ contient le groupe dérivé, donc est égal à $\mathfrak{A}_5$.

Simplicité de $\mathfrak{A}_n$

Il va falloir appliquer une variante du critère d'Iwasawa à l'action de $\mathfrak{A}_n$ sur l'ensemble des parties de $X = \{1, \ldots, n\}$ à k éléments, pour $k = 3$ ou $k = 4$.

Si S est une telle partie, on définit A_S comme

- le groupe alterné $\mathfrak{A}_S$ de cette partie si $k = 3$,
- le groupe des double transpositions à support dans cette partie si $k = 4$.

Ce sont des groupes commutatifs, isomorphes à $\mathrm{Z}/3\mathrm{Z}$ et $(\mathrm{Z}/2\mathrm{Z}) \times (\mathrm{Z}/2\mathrm{Z})$.

On a la relation $A_{g \cdot S} = g A_S g^{-1}$.

Leur réunion engendre $\mathfrak{A}_n$ (parce que les 3-cycles engendrent, ou bien les double transpositions).

Simplicité de $\mathfrak{A}_n$

Il va falloir appliquer une variante du critère d'Iwasawa à l'action de $\mathfrak{A}_n$ sur l'ensemble des parties de $X = \{1, \dots, n\}$ à k éléments, pour $k = 3$ ou $k = 4$.

Si S est une telle partie, on définit A_S comme

- le groupe alterné $\mathfrak{A}_S$ de cette partie si $k = 3$,
- le groupe des double transpositions à support dans cette partie si $k = 4$.

Ce sont des groupes commutatifs, isomorphes à $\mathrm{Z}/3\mathrm{Z}$ et $(\mathrm{Z}/2\mathrm{Z}) \times (\mathrm{Z}/2\mathrm{Z})$.

On a la relation $A_{g.S} = gA_Sg^{-1}$.

Leur réunion engendre $\mathfrak{A}_n$ (parce que les 3-cycles engendrent, ou bien les double transpositions).

Problème : l'action n'est pas 2-transitive.

Sommaire

Blocs

On appelle **bloc** de X une partie $B \subseteq X$ telle que pour tout $g \in G$, soit $B = g \cdot B$, soit $B \cap g \cdot B = \emptyset$.

```
/-- A block is a set which is either fixed or moved to a disjoint subset
    -/
def IsBlock (B : Set X) :=
  (Set.range fun g : G => g • B).PairwiseDisjoint id
```

Listing 4 – Définition d'un bloc en Lean

$B = \emptyset$, les singletons, $B = X$ sont des blocs, dits *triviaux* (prédicat `IsTrivialBlock`).

Actions primitives

Définition

Une action d'un groupe G sur un ensemble X est primitive si les seuls blocs sont les blocs triviaux.

```
/-- An action is preprimitive if it is pretransitive and the only blocks
    are the trivial ones -/
class IsPreprimitive [SMul G X] extends IsPretransitive G X : Prop where
  has_trivial_blocks' : ∀ {B : Set X}, IsBlock G B → IsTrivialBlock B
```

Listing 5 – Action primitive, Lean

Variante : les seules relations d'équivalences sur X qui sont compatibles avec l'action de G sont triviales (discrète ou grossière).

Introduit par Galois dans sa lettre à Auguste Chevalier : alors X est l'ensemble des racines d'un polynôme sur lequel agit le groupe de Galois G.

Transitivité et primitivité

- Une orbite est un bloc, donc *une action primitive est transitive.*

Transitivité et primitivité

- Une orbite est un bloc, donc *une action primitive est transitive.*
- *Une action 2-transitive est primitive.*
  Soit B un bloc non trivial.
  Soit $x, y \in B$, et soit $z \in X \setminus B$.
  Par 2-transitivité, il existe $g \in G$ tel que $g \cdot x = x$ et $g \cdot y = z$.
  Alors, $x \in B \cap g \cdot B$, donc $B = g \cdot B$.
  Comme $y \in B$ et $z = g \cdot y$, on a $z \in B$; contradiction.

Transitivité et primitivité

- Une orbite est un bloc, donc *une action primitive est transitive.*
- *Une action 2-transitive est primitive.*
  Soit B un bloc non trivial.
  Soit $x, y \in B$, et soit $z \in X \setminus B$.
  Par 2-transitivité, il existe $g \in G$ tel que $g \cdot x = x$ et $g \cdot y = z$.
  Alors, $x \in B \cap g \cdot B$, donc $B = g \cdot B$.
  Comme $y \in B$ et $z = g \cdot y$, on a $z \in B$; contradiction.
- *Dans une action primitive, tout sous-groupe distingué qui agit non trivialement agit transitivement.*
  Car l'orbite d'un point par un sous-groupe distingué est un bloc.

Actions primitives : géométrie

L'action de $\mathrm{SO}(3,\mathrm{R})$ *sur les droites de* R^3 *est*

- *transitive :* si u, v sont des vecteurs unitaires, il existe $g \in \mathrm{SO}(3,\mathrm{R})$ tel que $g \cdot u = v$.
- *non 2-transitive :* les rotations préservent les angles de droites
- mais est *primitive :* si un bloc contient (la droite passant par) le pôle nord et un autre point, il contient tout le parallèle correspondant, puis toute la sphère.

On en déduit que le groupe $\mathrm{SO}(3,\mathrm{R})$ est simple.

Actions primitives : géométrie

L'action de $\mathrm{SO}(3,\mathrm{R})$ *sur les droites de* R^3 *est*

- *transitive :* si u, v sont des vecteurs unitaires, il existe $g \in \mathrm{SO}(3,\mathrm{R})$ tel que $g \cdot u = v$.
- *non 2-transitive :* les rotations préservent les angles de droites
- mais est *primitive :* si un bloc contient (la droite passant par) le pôle nord et un autre point, il contient tout le parallèle correspondant, puis toute la sphère.

On en déduit que le groupe $\mathrm{SO}(3,\mathrm{R})$ est simple.

Cas général ? — Pour un groupe orthogonal « non compact », Tamagawa (1958)

Actions primitives : combinatoire

Si $n \geqslant 3$ et $k \neq 0, n/2, n$, l'action de $\mathfrak{A}_n$ sur les parties à k éléments de $\{1, \ldots, n\}$ est

- *transitive :* pour $a_1, \ldots, a_k$ et $b_1, \ldots, b_k$, prendre $g \in \mathfrak{S}_n$ tel que $g \cdot a_i = b_i$ pour tout i ; si nécessaire, composer avec une transposition $(b_1\ b_2)$ si $k \geqslant 2$, ou avec une transposition $(c\ c')$ si $n - k \geqslant 2$.
- *non 2-transitive :* on a $\mathrm{Card}(g \cdot A \cap g \cdot B) = \mathrm{Card}(A \cap B) \ldots$
- mais est *primitive*.

Simplicité de $\mathfrak{A}_n$

On en déduit une preuve un peu compliquée, mais « géométrique », de la simplicité de $\mathfrak{A}_n$:

- Si $n \geqslant 5$ et $n \neq 8$, prendre $k = 4$ et associer à une partie S de cardinal 4 le groupe des double transpositions à support dans S.
- Si $n \geqslant 5$ et $n \neq 6$, prendre $k = 3$ et associer à une partie S de cardinal 3 le groupe des permutations circulaires à support dans S.

Primitivité et maximalité

Proposition

Soit G un groupe agissant transitivement et non trivialement sur un ensemble X.

L'action de G sur X est primitive

$\Leftrightarrow$ *Pour tout $x \in X$, le stabilisateur G_x de x est un sous-groupe maximal de G.*

Plus généralement, les applications

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

sont des bijections croissantes entre l'ensemble des blocs de X contenant x et l'ensemble des sous-groupes de G contenant G_x.

Sous-groupes maximaux

Le critère d'Iwasawa justifie d'étudier systématiquement les sous-groupes maximaux d'un groupe (par exemple simple) donné. Cette étude est aussi une première étape d'une classification éventuelle des actions de groupes finis fondée sur la classification des groupes finis simples.

Ils sont explicités

- par un théorème de O'Nan–Scott (1980–81) pour le groupe symétrique/alterné ;
- par un théorème d'Aschbacher (1984) pour les groupes classiques sur un corps fini.

Le théorème de O'Nan et Scott pour le groupe alterné

Si G est un sous-groupe maximal de $\mathfrak{A}_n$, alors G est la trace sur $\mathfrak{A}_n$ d'un groupe de l'un des types suivants (à conjugaison près) :

- $G = \mathfrak{S}_k \times \mathfrak{S}_{n-k}$ pour $0 < k < n - k < n$
- $G = \mathfrak{S}_k \wr \mathfrak{S}_m$, où $n = mk$ et $m, k > 1$
- $n = p^k$ et G est le groupe affine de F_{p^k}

et trois autres cas...

Noter que ces groupes apparaissent comme des stabilisateurs de structures naturelles dans $\mathfrak{S}_n$: d'une partie, d'une partition, d'une bijection $\{1, \ldots, n\} \to \{1, \ldots, p\}^k$, etc.

La réciproque : Liebeck, Praeger, Saxl (1987)

Essentiellement, tous les sous-groupes maximaux proposés par O'Nan sont maximaux, avec quelques exceptions.

En particulier : si $1 \leqslant k < n/2$ (et $n \geqslant 5$), le stabilisateur d'une partie de cardinal k est un sous-groupe maximal de $\mathfrak{A}_n$. Autrement dit, l'action de $\mathfrak{A}_n$ sur les parties à k éléments de $\{1, \ldots, n\}$ est primitive.

C'est ce qu'il fallait pour conclure cette preuve pas très simple de la simplicité de $\mathfrak{A}_n$.

Preuve du résultat de primitivité

Proposition

Pour $k \in \mathbb{N}$ tel que $1 \leqslant k < n-k$ et $n \geqslant 5$, le sous-groupe $G = (\mathfrak{S}_k \times \mathfrak{S}_{n-k}) \cap \mathfrak{A}_n$ de $\mathfrak{A}_n$ est maximal.

Cas $k = 1$. Alors G est le stabilisateur de $\{1\}$, pour $n \geqslant 3$, l'action de $\mathfrak{A}_n$ sur $\{1, \ldots, n\}$ est 2-transitive donc primitive, donc G est maximal.

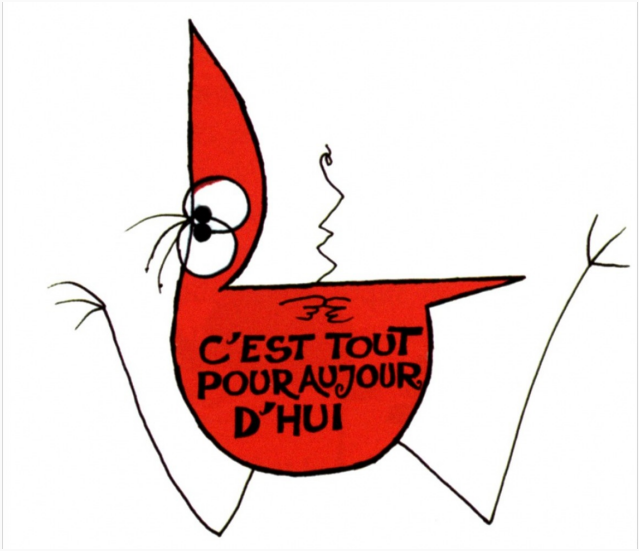
Cas $k \geqslant 2$. Soit H un groupe tel que $G < H \leqslant \mathfrak{A}_n$; on veut prouver $H = \mathfrak{A}_n$. On commence par prouver que H est primitif (c'est plutôt élémentaire, mais c'est là qu'on utilise que $k < n - k$!), et on conclut grâce à un théorème de Jordan (1870) : *un sous-groupe primitif de $\mathfrak{A}_n$ qui contient un 3-cycle est égal à $\mathfrak{A}_n$.*

Sommaire

Pourquoi « une expérience incomplète » ?

Plusieurs raisons :

- La preuve était complète sous `Lean` (version 3), il reste un petit bout à traduire en la version 4.
- Il faudra ensuite la pousser dans `mathlib`
- Cette preuve suggère de démontrer d'autres cas de simplicité suivant cette approche : groupes sporadiques et groupes géométriques.
- Pourquoi pas, formaliser les classifications des sous-groupes maximaux...


C'EST TOUT
POUR AUJOUR
D'HUI