Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$

Julie Parreaux

2018-2019

Référence du développement : Ulmer [4, p.53]

Leçons où on présente le développement : 104 (Groupes finis) ; 105 (Groupe symétrique) ; 108 (générateurs d'un groupe).

1 Introduction

L'objet de ce développement est de montrer la simplicité de $\mathfrak{A}_n$ dans le cas $n \geq 5$. Cependant, il est intéressant de noté que $\mathfrak{A}_n$ est simple pour $n \neq 4$, comme on va le voir ci-dessous.

Théorème 1. *Le groupe alterné $\mathfrak{A}_n$ est simple pour $n \neq 4$.*

Démonstration. Pour $n \leq 4$, on a naturellement :

- $\mathfrak{A}_1 = \mathfrak{S}_1 = \{Id\}$;
- $\mathfrak{A}_2 = \{Id\}$;
- $\mathfrak{A}_3$ est de cardinal 3 donc isomorphe à $\mathbb{Z}/_{3\mathbb{Z}}$ qui est simple ;
- $\mathfrak{A}_4$ n'est pas simple, car contient $V_4 = \{Id, (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ comme sous-groupe distingué non trivial (c'est le sous-groupe engendré par les doubles transpositions).

Le cas $n \geq 5$ est plus subtile et est donc l'objet de ce développement. □

2 Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$

Le théorème que l'on souhaite montrer dans le développement est le suivant (on remarque que c'est la partie la plus technique de la preuve du théorème introduit précédemment) :

Théorème 2. *Le groupe $\mathfrak{A}_n$ est alterné quand $n \geq 5$.*

Schéma du développement

1. Les 3-cycles engendrent le groupe alterné $\mathfrak{A}_n$, quand $n \geq 5$.
   (a) Les trois cycles sont dans $\mathfrak{A}_n$.
   (b) Tout élément de $\mathfrak{A}_n$ s'écrit comme un produit pair de transposition.
   (c) Un produit de deux transpositions s'écrit comme un produit de 3-cycles.
2. Les 3-cycles sont conjugués entre eux dans $\mathfrak{A}_n$, quand $n \geq 3$: étude de la bonne permutation avec des commutateurs.
3. Preuve du théorème.
   (a) Si H contient un 3-cycle alors $H = \mathfrak{A}_n$.
   (b) Si H contient un p-cycle γ où $p \geq 4$, alors $H = \mathfrak{A}_n$.
   (c) Si H ne contient que des 2-cycles, alors on a une contradiction.

Lemme 1. *Les 3-cycles engendrent le groupe alterné $\mathfrak{A}_n$ (quand $n \geq 3$).*

Démonstration. L'hypothèse $n \geq 3$ permet d'assurer l'existence des 3-cycles.

La signature d'un trois cycle est $(-1)^{n-(n-2)} = 1$ (car il y a $n-3$ orbites réduites à un singletons et une orbite de taille 3, par définition d'un 3-cycle). Donc l'ensemble des 3-cycles est inclus dans $\mathfrak{A}_n$.

Tout élément de $\mathfrak{A}_n$ est le produit d'un nombre paire de transpositions. (En effet,les transpositions engendrent $\mathfrak{S}_n$ et comme la signature d'une transposition vaut -1 (car on a $(-1)^{n-(n-1)} = -1$), tous les éléments de $\mathfrak{A}_n$ s'écrivent comme produit d'un nombre de transposition qui doit être paire pour obtenir la bonne signature.

Un produit de deux transpositions est soit un 3-cycle, soit un produit de 3-cycles :

$$\begin{cases} (i,j)(k,l) = (i,l,k)(i,j,k) \\ (i,j)(i,k) = (i,k,j) \end{cases}$$

Ce qui conclut la preuve. □

Définition 1 (Éléments conjugués)**.** Deux éléments γ, γ' de $\mathfrak{A}_n$ sont dits conjugués s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma\gamma\sigma^{-1} = \gamma'$.

Lemme 2. *Les 3-cycles sont conjugués entre eux dans $\mathfrak{A}_n$, quand $n \geq 5$.*

Démonstration. Soit (i,j,k) un 3-cycle quelconque de $\mathcal{S}_n$. On introduit la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & s & \dots & \end{pmatrix}$$

où $l, s \in \{1, \dots, n\} \setminus \{i,j,k\}$ (on utilise ici l'hypothèse $n \geq 5$ pour trouver l et s tels qu'on les souhaite).

L'une des deux transpositions σ ou $\sigma' = \sigma \circ (l,s)$ est paire donc appartient à $\mathfrak{A}_n$. (En effet, si σ n'est pas paire, alors sa signature vaut -1 et comme la signature d'une transposition vaut -1 et que la signature est un morphisme de groupe, alors la signature de σ' vaut 1 : elle est donc paire. Sinon, σ est déjà paire.)

De plus, $\sigma(1,2,3)\sigma^{-1} = \sigma'(1,2,3)\sigma'^{-1} = (i,j,k)$ (car ls n'agit dans le support de σ). Donc (i,j,k) et $(1,2,3)$ sont conjugués. Par transitivité de la relation de conjugaison (en effet, soit α, β, γ, trois transpositions de $\mathfrak{S}_n$ telles que α et β soient conjuguées ainsi que β et γ. Alors, il existe $\sigma, \sigma' \in \mathfrak{S}_n$ telles que $\alpha = \sigma\beta\sigma^{-1}$ et $\beta = \sigma'\gamma\sigma'^{-1}$, soit $\alpha = \sigma\sigma'\gamma\sigma'^{-1}\sigma^{-1}$ d'où le résultat), on en déduit que deux 3-cycles sont toujours conjugués dans $\mathfrak{A}_n$ (en effet, soit deux 3-cycles, par ce qui précèdent, on peut toujours les conjuguer à $(1,2,3)$ et conclure par transposition). □

Théorème 3. *Le groupe $\mathfrak{A}_n$ est alterné quand $n \geq 5$.*

Démonstration. Soit H un sous-groupe distingué de $\mathfrak{A}_n$ distinct de $\{Id\}$. On distingue tous les cas possibles.

Si H contient un 3-cycle : donc, d'après le lemme 2 (on utilise ici l'hypothèse $n \geq 5$ puisque nous utilisons le lemme 2), il les contient tous. Comme les 3-cycles engendrent $\mathfrak{A}_n$ (lemme 1), on en déduit que $H = \mathfrak{A}_n$.

Si H contient un p-cycle γ où $p \geq 4$: supposons, sans perte de généralité que $\gamma = (1,2,\dots,p)$. Soit $\nu = (1,2,3)$. Alors $\nu^{-1} = (1,3,2)$ et $\gamma^{-1} = (1,p,p-1,\dots,2)$ (se vérifie par un calcul rapide) et on vérifie que $\gamma^{-1}\nu^{-1}\gamma\nu = (2,3,p)$ (nécessite de faire proprement le calcul).

Comme $H \lhd A_n$, $\gamma \in H \Rightarrow (\gamma^{-1} \in H$ et $\nu^{-1}\gamma\nu \in H) \Rightarrow (2,3,p) \in H$ (par les propriétés de groupe pour H et car H est distingué dans $\mathfrak{A}_n$). Donc H contient un 3-cycle et le premier point donne $H = \mathfrak{S}_n$ (on utilise ici l'hypothèse $n \geq 5$ puisque nous utilisons le point précédent).

Si H ne contient que des 2-cycles : soit $\sigma \in H \setminus \{Id\}$, σ est le produit d'un nombre pair de transposition : $\sigma = (i,j)(k,l)\dots$. Cette décomposition est en fait la décomposition de σ en produit de cycles à supports disjoints (les cycles à supports disjoints engendrent $\mathfrak{S}_n$), de sorte que toutes les transpositions

qui interviennent dans le produit $\sigma = (i,j)(k,l)\dots$ après les deux premières ont des supports qui n'intersectent pas $\{i,j,k,l\}$. Si on note, $\sigma = (i,j)(k,l)\phi$, on a $Supp(\phi) \cap \{i,j,k,l\} = \emptyset$. Si $\nu = (i,j,k)$ alors $\nu^{-1}\sigma\nu\sigma^{-1} = (i,l)(j,k)$.

Mais $H \lhd A_n$, donc $\nu^{-1}\sigma\nu \in H$ ($\sigma \in H$) et comme $\sigma^{-1} \in H$ (H est un groupe), alors $\nu^{-1}\sigma\nu\sigma^{-1} \in H$, soit $(i,l)(j,k) \in H$. H contient alors un produit de deux transpositions.

On peut donc supposer que H contient le produit $\sigma = (i,j)(k,l)$. Soit $s \notin \{i,j,k,l\}$ et $\beta = (k,l,s)$, alors $\beta^{-1}\sigma\beta\sigma^{-1} = \beta$ (on utilise ici l'hypothèse $n \geq 5$ pour trouver le s qui convient). Mais H étant distingué dans $\mathfrak{A}_n$, $\beta^{-1}\sigma\beta \in H$ et comme précédemment, $\beta \in H$.

Absurde car H ne contient pas de trois cycles par hypothèse. D'où le théorème. □

Remarque : Les produit comme celui-ci : $\beta^{-1}\sigma\beta\sigma^{-1}$, s'appelle des commutateurs.

3 Compléments autours de la simplicité d'un groupe

Quelques applications

Nous donnons ici quelques applications de la simplicité de $\mathfrak{A}_n$ quand $n \neq 4$.

Proposition 1 (Application 1.). *Pour $n \neq 4$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Idée de la preuve. On se donne un sous-groupe distingué et on fait son intersection avec $\mathfrak{A}_n$ qui donne soit $\{Id\}$ soit $\mathfrak{A}_n$ et on conclut par une distinction de cas. □

Proposition 2 (Application 2.). *Il n'y a pas de surjection de $\mathfrak{S}_n$ dans $\mathfrak{S}_{n+1}$ pour $n \geq 5$.*

Idée de la preuve. On raisonne par l'absurde. □

Sous-groupe distingué

Les sous-groupes distingués sont les sous-groupes qui permettent de définir les groupes quotients [3, p.18]. En effet, lorsqu'on fait la quotient d'un groupe par un sous-groupe, le quotient est groupe si et seulement si le sous-groupe est distingué.

Définition 2 (Sous-groupe distingué)**.** Un sous-groupe H de G est distingué (ou normal) dans G si $xH = Hx$ pour tout $x \in G$. On note alors $H \lhd G$.

Remarque : Les sous-groupes distingués peuvent être aussi défini à l'aide des automorphismes intérieurs.

Proposition 3 (Caractérisation des sous-groupes distingués)**.** *Soit H un sous-groupe distingué de G. Les propriétés suivantes sont équivalentes.*

1. $\forall x \in G,\ xH = Hx$
2. $\forall x \in G,\ xH \subseteq Hx$
3. $\forall x \in G,\ xHx^{-1} = H$
4. $\forall x \in G,\ xHx^{-1} \subseteq H$

Démonstration. On a 1 qui est équivalent à 3 et 2 équivalent à 4. De plus 1 implique 2, montrons la réciproque. Comme $xH \subseteq Hx$ pour n'importe quel $x \in G$, alors $x^{-1}H \subseteq Hx^{-1}$. En particulier $x(x^{-1}H)x \subseteq x(Hx^{-1})x$ d'où l'inclusion manquante. □

Théorème 4. *Soit $f : G \to G'$ un morphisme de groupes. Soient H et H' des sous-groupes respectifs de G et de G'. Alors :*

1. $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$;
2. $H \lhd G \Rightarrow f(H) \lhd f(G)$;

Démonstration. Soit $f : G \to G'$ un morphisme de groupes. Soient H et H' des sous-groupes respectifs de G et de G'.

1. Soit $g \in G$, $x \in f^{-1}(H')$ et montrons que $gxg^{-1} \in f^{-1}(H')$. Comme $H' \lhd G'$, $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) \in H'$ (f est un morphisme de groupe). Donc, par définition de l'application inverse $gxg^{-1} \in f^{-1}(H')$.
2. Soit $g \in G$, $h \in H$, montrons que $f(g)f(h)f(g)^{-1} \in f(H)$. Comme f est un morphisme et que H est distingué dans G, on obtient le résultat immédiatement.

□

Lemme 3. *Si H et K sont deux sous-groupes de G, alors :*

1. *si $H \lhd G$, alors $HK = KH$ est un sous-groupe de G ;*
2. *si $H \lhd G$ et $K \lhd G$, alors $HK \lhd G$.*

Démonstration. Soient H et K sont deux sous-groupes de G

1. Se montre en écrivant la définition de distingué.
2. $\forall g \in G, gHK = HgK = HKg$.

□

Théorème 5 (Deuxième théorème d'isomorphisme)**.** *Soit H un sous-groupe distingué d'un groupe G, et K un sous-groupe de G. Alors,*

1. $K \cap H \lhd K$;
2. $H \lhd KH$;
3. $K/K \cap H \simeq KH/H$.

Démonstration. Soit H un sous-groupe distingué d'un groupe G, et K un sous-groupe de G.

1. Soit $h \in K \cap H$ et $k \in K$, montrons que $khk^{-1} \in K \cap H$. Dans K par produit d'éléments de K (K est un groupe). Dans H car H est distingué dans G.
2. On a $H \subseteq KH \subseteq G$ et H distingué dans G, ce qui implique le résultat en revenant aux différentes définitions.
3. L'application $\begin{array}{rccc} f : & K & \to & KH/H \\ & k & \mapsto & \dot{k} \end{array}$ est un morphisme. Il est surjectif car un élément de $KH = HK$ est de la forme hk et $\dot{hk} = \dot{k}$ (car $(hk)k^{-1} \in H$). Comme $\ker f = K \cap H$, on a bien le résultat (par décomposition canonique).

□

Théorème 6 (Troisième théorème d'isomorphisme)**.** *Soit H un sous-groupe distingué d'un groupe G. On note $\pi : G \to G/H$ la projection canonique.*

1. *Les sous-groupes distingués de G/H sont de la forme K/H où K est un sous-groupe de G tel que $H \subset K \lhd G$. L'application $\begin{array}{rccc} \Psi : & \mathcal{G} & \to & \mathcal{G}' \\ & K & \mapsto & \pi(k) = K/H \end{array}$ est une bijection croissante de l'ensemble $\mathcal{G}$ des sous-groupes distingués de G contenant H sur l'ensemble $\mathcal{G}'$ des sous-groupes distingués de G/H.*
2. *Si $H \subset K \lhd G$, alors $(G/H)/(K/H) \simeq G/K$.*

Démonstration. Soit H un sous-groupe distingué d'un groupe G. On note $\pi : G \to G/H$ la projection canonique.

1. L'application Ψ est bien défini car $\pi(K)$ est un sous-groupe distingué comme image par un morphisme de groupe (ici, on parle de π) d'un sous-groupe distingué. Elle est surjective par surjectivité de π et comme l'image réciproque d'un sous-groupe distinguée est distinguée. L'injectivité s'établie par double inclusion.
2. L'application $\begin{array}{rccc} \psi : & G/H & \to & G/H \\ & \dot{x} & \mapsto & \bar{x} \end{array}$ est bien définie et sa décomposition canonique donne l'isomorphisme recherché.

□

Définition 3 (Groupe simple)**.** Un groupe est dit simple s'il n'admet pas de sous-groupe distingué propre, c'est-à-dire autre de $\{id\}$ et lui-même.

Application (Troisième théorème d'isomorphisme aux groupes simples) : Étant donné H un sous-groupe distingué de G maximal dans l'ensemble des sous-groupes distingué de G (distinct de G), on montre (par le troisième théorème d'isomorphisme) que G/H est simple. (En effet, K/H sera distingué dans G/H si et seulement si $H \subseteq K \lhd G$, ce qui équivaut ici à $K = H$ ou G soit $K/H = \{\dot{e}\}$ ou G/H.) On a alors la relation suivante : G/H simple $\Leftrightarrow$ H sous-groupe distingué maximal de G.

Théorème 7 (Quotient d'un groupe [2, p.150])**.** *Soit H un sous-groupe distingué de G, alors l'ensemble quotient $G \setminus H$ peut être muni d'une loi interne quotient induite par celle de G, telle que $\forall \overline{x}, \overline{y} \in G \setminus H$, $\overline{x}\,\overline{y} = \overline{xy}$. Muni de cette loi, $G \setminus H$ a une structure de groupe.*

Définition 4. Si H un sous-groupe distingué de G, alors le groupe $G \setminus H$ est appelé groupe quotient.

Orbites, transpositions et cycles

On va alors définir la notion d'orbite qui est l'orbite de l'action de $\mathfrak{S}_n$ sur un ensemble fini à n éléments [1, p.204]. De cette notion, on caractérise les transpositions et les cycles qui jouent un rôle important dans le groupes (ce sont des système de générateur). On se place dans le cas où E contient un ensemble fini d'élément $n \geq 2$.

Soit $\sigma \in \mathfrak{S}(E)$. L'action naturelle de $\mathfrak{S}(E)$ sur E se restreint en un action du sous-groupe $\langle \sigma \rangle$ sur E. Une orbite de cette action est appelée une σ-orbite que nous notons Orb_σ.

Définition 5. Soient $\sigma \in \mathfrak{S}(E)$ et $x \in E$, la σ-orbite de x est définie comme l'ensemble $\mathrm{Orb}_\sigma(x) = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$.

Lemme 4. *Quelques propriétés des orbites :*

1. $\mathrm{Orb}_\sigma(x)$ *est réduite à un singleton si et seulement si* x *est un point fixe de* σ.
2. *Les différentes* σ*-orbites de* E *forment une partition de* E.
3. *La réunion* σ*-orbites non réduite à un singleton est égale au support de* σ.

Démonstration. 1. x est un point fixe $\Leftrightarrow \sigma(x) = x \Leftrightarrow \sigma^m(x) = x \Leftrightarrow \mathrm{Orb}_\sigma(x)$ est réduite à un singleton.
2. Formule des classes de l'action naturelle de $\mathfrak{S}(E)$.
3. $x \in \mathrm{Supp}(\sigma) \Leftrightarrow \sigma$ n'est pas un point fixe $\Leftrightarrow$ la réunion σ-orbites non réduite à un singleton.

□

Proposition 4. *Soit* $\sigma \in \mathfrak{S}(E)$ *une permutation, soit* w *une* σ*-orbite à* p *éléments, et soit* $a \in w$. *Alors* p *est le plus entier strictement positif tel que* $\sigma^p(a) = a$, *et l'on a* $w = \{a, \sigma(a), \ldots, \sigma^{p-1}(a)\}$.

Démonstration. $\mathfrak{S}(E)$ est fini, tout sous-groupe est d'indice fini. □

Définition 6. On appelle cycle toute permutation σ dont une et une seule orbite n'est pas réduite à un singleton. Cette orbite est le support du cycle, et le cardinal de ce support est appelée la longueur du cycle.

Définition 7. On appelle transposition tout cycle de longueur 2. Autrement dit, une transposition de $\mathfrak{S}(E)$ a $n-2$ points fixes et échange deux éléments.

Lemme 5. *Un* p*-cycle est d'ordre* p.

Démonstration. Soit $\sigma = (a_1 \ \ldots \ a_p)$, $\forall j \in [\![1, p-1]\!]$, $\sigma^j(a_1) = a_{j+1} \neq a_1$. De plus $\sigma^p = Id_E$, car $\forall k \in [\![1, p]\!]$, $\sigma^p(a_k) = a_k$. □

Application : L'inverse d'une transposition est elle-même.

Le groupe alterné

Nous allons définir la signature qui nous permet de définir le groupe alterné [1, p.215].

Théorème 8. *Soit* E *un ensemble fini à plus de deux éléments. Alors il existe un unique morphisme* $\epsilon(\sigma) : \mathfrak{S}_n \to \mathbb{C}^\times$ *non trivial. Si* $\sigma \in \mathfrak{S}(E)$ *s'écrit comme* s *produit de transpositions, alors on a* $\epsilon(\sigma) = (-1)^s$.

Démonstration. Soit ϵ un morphisme de groupe : $\mathfrak{S}_n \to \mathbb{C}^\times$ non trivial. Alors ϵ est constant sur les classes de conjugaison de $\mathfrak{S}(E)$. Si τ est une transposition $\epsilon(\tau) = -1$ et $\epsilon(\tau^s) = (-1)^s$. □

Définition 8. Si $\sigma \in \S_n(E)$, l'élément $\epsilon(\sigma)\{-1; 1\}$ est appelé signature de σ.

Interprétation : On peut aussi la voir comme le nombre d'orbite d'une permutation (comme définit précédemment) Dans, ce cas $\epsilon(\sigma) = (-1)^{n-w}$ où w est le nombre d'orbites de σ.

Proposition 5. *Soit* E *un ensemble à* n *éléments, et soit* $\sigma \in \Sigma_n(E)$. *Alors,* $\epsilon(\sigma) = (-1)^{n-N_\sigma}$ *où* N_σ *est le nombre de* σ*-orbites.*

Démonstration. Soit σ que l'on décompose en cycle. On peut alors en déduire le nombre de points fixes ce qui nous permet de compter le nombre de σ-orbites. □

Définition 9. Le groupe alterné de degré n, noté $\mathfrak{A}_n$, est le sous-groupe distingué de $\mathfrak{S}_n$ tel que la signature de ces éléments vaut 1. On dit que $\mathfrak{A}_n$ contient les permutations paires (les permutations impaires sont dans $\mathfrak{S}_n \setminus \mathfrak{A}_n$).

Remarque : Une autre manière de le voir est de dire que $\mathfrak{A}_n$ est le noyau du morphisme de signature qui est bien un sous-groupe distingué. On voit alors immédiatement que l'indice de $\mathfrak{A}_n$ est 2, donc il est distingué.

Proposition 6. *Le cardinal de* $\mathfrak{A}_n$ *est* $\frac{n!}{2}$. *Démonstration.* Il existe uniquement deux classes seules classes à gauche. □

Proposition 7. *Soit* E *un ensemble ayant au moins deux éléments. Alors, le groupe alterné* $\mathfrak{A}(E)$ *est l'unique sous-groupe d'indice deux de* $\mathfrak{S}(E)$.

Démonstration. On définit un morphisme. On utilise le caractère distingué pour conclure. □

Proposition 8. *Soit* E *un ensemble à* n *éléments. Si* $n \geq 3$, *le groupe alterné* $\mathfrak{A}(E)$ *est engendré par chacune des familles suivantes :*
1. *les produits de deux transpositions ;* 2. *les* 3*-cycles.*

Démonstration. 1. Comme $\epsilon(\sigma) = 1$, il faut un nombre pair de transposition pour décomposé σ.

2. On montre que le produit de deux transpositions est un 3-cycle.

□

Théorème 9. *$\mathfrak{A}_n$ est simple pour $n \neq 4$.*

Remarque : Le sous-groupe engendré par les double transpositions est un sous-groupe distingué de $\mathfrak{A}_4$.

Corollaire 1. *Soit E un ensemble à n éléments ($n \geq 2$). Si $n \neq 4$, les sous-groupes distingués de $\mathfrak{S}(E)$ sont $\{Id_E\}$, $\mathfrak{A}(E)$ et $\mathfrak{S}(E)$.*

Démonstration. Soit H un sous-groupe distingué de $\mathfrak{S}(E)$, donc $\mathfrak{A}(E) \cap H$ est distingué. On a $\mathfrak{A}(E) \cap H = \{Id_E\}$ ce qui induit une signature injective et $H = \{Id_E\}$. On a $\mathfrak{A}(E) \cap H = \mathfrak{A}(E)$, dans ce cas H contient deux classes à gauche distincte et $H = \mathfrak{A}(E)$. □

Références

[1] G. Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[2] J. Calais. *Éléments de la théorie des groupes*. puf, 1984.

[3] D. J. Mercier. *Fondamentaux d'algèbre et d'arithmétique*. CSIPP, 2015.

[4] F. Ulmer. *Théorie des groupes*. ellipses, 2012.