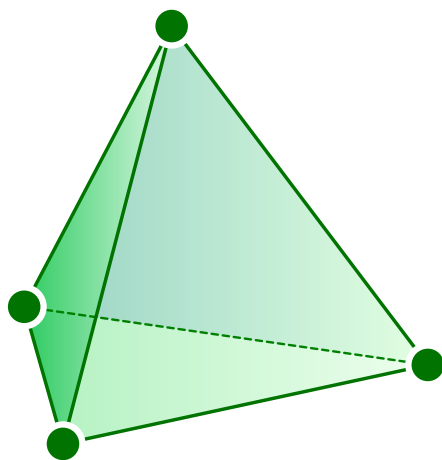


MÉMOIRE DE MATHÉMATIQUES

Sorbonne Université — Licence 2

Du simplexe à la simplicité, une promenade autour du groupe alterné

Action de $\mathfrak{S}_{n+1}$ sur Δ_n et simplicité de $\mathcal{A}_n$



Auteurs

Thomas DOUCY

Maxime ETCHEGARAY

Sous la direction de Baptiste DUGUÉ

Juin — Juillet 2026

Table des matières

1	Action du groupe symétrique $\mathfrak{S}_{n+1}$ sur le simplexe Δ_n	2
1.1	Lemme de convexité	2
1.2	Interlude : groupe symétrique	4
1.3	Le cas $n = 3$: le tétraèdre	6
1.3.1	Action de $\mathfrak{S}_4$ sur le tétraèdre	6
1.3.2	Étude géométrique	8
1.4	Le cas général : le simplexe	10
2	Simplicité de $\mathcal{A}_n$	12
2.1	Simplicité d'un groupe	12
2.2	Les cas $n = 1, 2$ et 3	13
2.3	Le cas $n = 4$: l'exception	14
2.3.1	Non-simplicité de $\mathcal{A}_4$	14
2.3.2	Complément : le groupe de Klein	16
2.4	Le cas $n = 5$	16
2.4.1	Corps finis	16
2.4.2	Caractère isomorphe de $\mathrm{SL}_2(\mathbb{F}_4)$ et $\mathcal{A}_5$	18
2.4.3	Simplicité de $\mathrm{SL}_2(\mathbb{F}_4)$	28
2.4.4	Conclusion	37

Dans toute la suite, n désigne un entier naturel non-nul.

Chapitre 1

Action du groupe symétrique $\mathfrak{S}_{n+1}$ sur le simplexe Δ_n

1.1 Lemme de convexité

Définition 1.1. Soient $x, y \in \mathbb{R}^n$. On appelle segment $[x, y]$ l'ensemble

$$[x, y] = \{x + t(y - x) \mid 0 \leq t \leq 1\}.$$

Définition 1.2. On munit $\mathbb{R}^n$ du produit scalaire usuel. On définit le groupe orthogonal de $\mathbb{R}^n$ par

$$O(\mathbb{R}^n) = \{f \in \mathcal{L}(\mathbb{R}^n) \mid \forall x, y \in \mathbb{R}^n, \langle f(x), f(y) \rangle = \langle x, y \rangle\}.$$

C'est un sous-groupe du groupe linéaire $GL(\mathbb{R}^n)$.

Définition 1.3. On munit $\mathbb{R}^n$ du produit scalaire usuel et on considère X une partie de $\mathbb{R}^n$. Une isométrie vectorielle de X est un élément de $O(\mathbb{R}^n)$ qui vérifie

$$\boxed{f(X) = X}$$

On note $\text{Isom}(X)$ l'ensemble des isométries vectorielles de X , qui est un sous-groupe de $O(\mathbb{R}^n)$.

Remarque 1.4. Soit X une partie de $\mathbb{R}^n$, on a $\text{Isom}(X) < O(\mathbb{R}^n) < GL(\mathbb{R}^n)$.

Propriété 1.5.

Soit X une partie de $\mathbb{R}^n$. Tout élément $f \in \text{Isom}(X)$ induit une bijection $f|_X$ de X dans X .

Démonstration.

Soit $f \in \text{Isom}(X)$. Par définition, f est un automorphisme de $\mathbb{R}^n$ vérifiant de plus $f(X) = X$. On peut donc considérer sa restriction à X , notée $f|_X$: elle est surjective puisque $f|_X(X) = f(X) = X$, et injective en tant que restriction d'une application injective. C'est donc une bijection de X dans X . $\square$

Lemme 1.6.

Soit C un convexe de $\mathbb{R}^n$, alors

$$\forall f \in \text{Isom}(C), \forall (a, b) \in C^2, f([a, b]) = [f(a), f(b)].$$

Démonstration.

Soient $f \in \text{Isom}(C)$ et $a, b \in C$. Pour tout $x \in [a, b]$, la convexité de C assure que x appartient encore à C . On s'intéresse donc à la restriction $f|_C$ de f à C , qui est une bijection de C dans lui-même d'après la propriété 1.5. Comme

$$\forall x \in C, f|_C(x) = f(x),$$

on écrira simplement f pour alléger les notations. On a alors

$$\begin{aligned} & f(x) \in f([a, b]) \\ \iff & x \in [a, b] \text{ par injectivité de } f|_C \\ \iff & \exists t_x \in [0, 1], x = a + t_x(b - a) \\ \iff & \exists t_x \in [0, 1], f(x) = f(a + t_x(b - a)) \text{ par bijectivité de } f|_C \\ \iff & \exists t_x \in [0, 1], f(x) = f(a) + t_x(f(b) - f(a)) \text{ par linéarité de } f \\ \iff & f(x) \in [f(a), f(b)] \end{aligned}$$

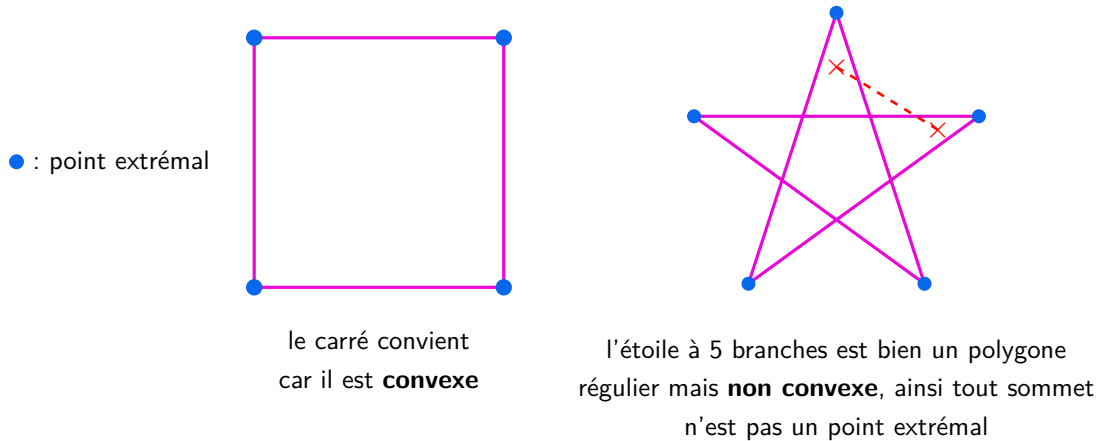
ceci assure que $f([a, b]) = [f(a), f(b)]$. □

Définition 1.7. Soit C un convexe de $\mathbb{R}^n$. On dit que $x \in C$ est un point extrémal de C si et seulement si

$$\forall (y, z) \in C^2, x \in [y, z] \implies x = y \text{ ou } x = z.$$

On note $\text{Ext}(C)$ l'ensemble de ces points.

Remarque 1.8. Pour un polygone régulier **convexe** quelconque de $\mathbb{R}^2$, ses points extrémaux sont exactement ses sommets :



Le lemme précédent permet alors de prouver le théorème suivant :

Théorème 1.9 (Lemme de convexité).

Soit C un convexe de $\mathbb{R}^n$, alors $\mathcal{Ext}(C)$ est stable par $\text{Isom}(C)$, i.e.

$$\forall f \in \text{Isom}(C), \forall x \in \mathcal{Ext}(C), f(x) \in \mathcal{Ext}(C).$$

Démonstration.

Soient $x \in \mathcal{Ext}(C)$ et $f \in \text{Isom}(C)$. Soit $(y, z) \in C^2$ et supposons que $f(x) \in [y, z]$.

La bijectivité de $f|_C$ fournit un unique couple $(\alpha, \beta) \in C^2$ vérifiant

$$\begin{cases} y = f(\alpha) \\ z = f(\beta) \end{cases},$$

d'où $f(x) \in [f(\alpha), f(\beta)]$.

Le lemme précédent donne alors $x \in [\alpha, \beta]$, et comme x est extrémal, on a $x = \alpha$ ou $x = \beta$.

En appliquant f , il vient

$$f(x) = f(\alpha) = y \text{ ou } f(x) = f(\beta) = z.$$

Nous avons ainsi établi que

$$\forall (y, z) \in C^2, f(x) \in [y, z] \implies f(x) = y \text{ ou } f(x) = z,$$

ce qui signifie exactement que $f(x)$ est extrémal, autrement dit $f(x) \in \mathcal{Ext}(C)$.

□

1.2 Interlude : groupe symétrique

Nous rappelons ici quelques notions et résultats sur le groupe symétrique, qui nous seront utiles par la suite.

Notation 1.10. On note $\mathfrak{T}_n$ l'ensemble des transpositions de $\mathfrak{S}_n$. Plus précisément,

$$\mathfrak{T}_n = \{(i \ j) \mid 1 \leq i \neq j \leq n\}.$$

Théorème 1.11.

Toute permutation de $\mathfrak{S}_n$ peut se décomposer en un produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.

Proposition 1.12.

Soit $\sigma = (i_1 \ i_2 \ \dots \ i_k)$ un k -cycle, on peut décomposer σ en produit de transpositions de la manière suivante :

$$\sigma = (i_1 \ i_2)(i_2 \ i_3) \dots (i_{k-1} \ i_k)$$

Ces deux résultats se combinent en un théorème fondamental :

Théorème 1.13.

$\mathfrak{S}_n$ engendre $\mathfrak{S}_n$.

Démonstration.

Soit $\sigma \in \mathfrak{S}_n$. Le théorème 1.11 décompose σ en un produit de cycles à supports disjoints, que la proposition 1.12 décompose à leur tour en produits de transpositions. Une telle décomposition de σ existe donc, mais elle est loin d'être unique : il en existe même une infinité. $\square$

Proposition 1.14.

Il existe un unique morphisme de groupes non trivial de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$, dit morphisme signature, défini par

$$\forall \sigma \in \mathfrak{S}_n, \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Remarque 1.15. On montre aisément que toute transposition τ de $\mathfrak{S}_n$ vérifie $\varepsilon(\tau) = -1$. La signature d'une permutation ne dépend donc que de la parité du nombre de transpositions apparaissant dans sa décomposition selon $\mathfrak{S}_n$.

Définition 1.16. On définit le groupe alterné de taille n comme étant le noyau de la signature, soit

$$\mathcal{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\} = \ker \varepsilon$$

Par construction, $\mathcal{A}_n$ est un sous-groupe de $\mathfrak{S}_n$, de cardinal $\frac{n!}{2}$.

Définition 1.17. Soit $\sigma \in \mathfrak{S}_n$ et k un entier. On définit le type de σ par la donnée du nombre de 1-cycles, de 2-cycles, ..., de n -cycles dans sa décomposition en produit de cycles à supports disjoints. Si σ se décompose en k cycles, en ordonnant les cycles par ordre décroissant de longueur, le i -ème cycle étant de longueur ℓ_i , on note

$$\text{type}(\sigma) = (\ell_1, \dots, \ell_k),$$

établissant ainsi la convention $\ell_1 \geq \dots \geq \ell_k$.

Exemple 1.18. La permutation $\sigma = (1 \ 3 \ 4)(2 \ 5)$ de $\mathfrak{S}_5$ est de type $(3, 2)$. Vue dans $\mathfrak{S}_8$ en revanche, elle s'écrit $\sigma = (1 \ 3 \ 4)(2 \ 5)(6)(7)(8)$, et son type devient $(3, 2, 1, 1, 1)$.

Remarque 1.19. La décomposition en cycles à supports disjoints impose que

$$\ell_1 + \dots + \ell_k = n$$

Déterminer tous les types possibles que peut prendre une permutation de $\mathfrak{S}_n$ revient donc à déterminer les partitions de l'entier n .

1.3 Le cas $n = 3$: le tétraèdre

1.3.1 Action de $\mathfrak{S}_4$ sur le tétraèdre

Définition 1.20. Soit $n, m \in \mathbb{N}^*$ et $\mathcal{F} = (e_1, \dots, e_m)$ une famille de vecteurs de $\mathbb{R}^n$. On définit l'enveloppe convexe de $\mathcal{F}$ comme l'intersection de tous les convexes contenant $\mathcal{F}$. Il s'agit donc du "plus petit" convexe contenant $\mathcal{F}$.

Définition 1.21. Soit $B = (e_1, e_2, e_3, e_4)$ la base canonique de $\mathbb{R}^4$. Le tétraèdre régulier, noté Δ_3 , est défini comme l'enveloppe convexe de B .

Définition 1.22. Soit X un ensemble, soit $(G, *)$ un groupe de neutre e . Soit

$$\begin{aligned} \alpha : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

une application de $G \times X$ dans X . On dit que α est une action de G sur X si elle vérifie :

- i) $\forall x \in X, \alpha(e, x) = e \cdot x = x$
- ii) $\forall (g, h) \in G^2, \forall x \in X, g \cdot (h \cdot x) = (g * h) \cdot x$

Cette définition est équivalente à la donnée d'un morphisme de groupes

$$\phi : (G, *) \longrightarrow (\mathfrak{S}(X), \circ),$$

ces deux définitions étant liées par

$$\forall g \in G, \forall x \in X, g \cdot x = (\phi(g))(x).$$

Si le morphisme ϕ est injectif, on dira que l'action est fidèle.

Théorème 1.23.

On considère le morphisme

$$\begin{aligned} \varphi : (\text{Isom}(\Delta_3), \circ) &\longrightarrow (\mathfrak{S}_4, \circ) \\ f &\longmapsto \sigma_f \end{aligned},$$

où pour tout $1 \leq i \leq 4$, $\sigma_f(i) = j$ avec j vérifiant $f(e_i) = e_j$.

Le morphisme φ est bijectif.

Démonstration.

Pour établir que φ est un isomorphisme, nous montrons qu'il est à la fois surjectif et injectif.

Surjectivité :

Montrons d'abord que toute transposition de $\mathfrak{S}_4$ est l'image par φ d'une isométrie de Δ_3 . Par construction, $\text{Isom}(\Delta_3) \curvearrowright \Delta_3$. Or, Δ_3 est une enveloppe convexe : il est donc entièrement déterminé par ses points extrémaux, qui ne sont autres que les vecteurs de la base

canonique de $\mathbb{R}^4$. Par ailleurs, le lemme de convexité a établi que

$$\forall f \in \text{Isom}(\Delta_3), f(\mathcal{Ext}(\Delta_3)) \subset \mathcal{Ext}(\Delta_3).$$

ce qui permet d'affirmer que l'action de $\text{Isom}(\Delta_3)$ sur Δ_3 induit une action sur $\mathcal{Ext}(\Delta_3)$, i.e. :

$$\boxed{\text{Isom}(\Delta_3) \curvearrowright \mathcal{Ext}(\Delta_3)}$$

Une isométrie de Δ_3 est donc entièrement déterminée par son action sur les seuls points extrémaux.

Considérons alors la symétrie $s \in \text{Isom}(\Delta_3)$ par rapport au plan passant par e_i, e_j et le milieu de $[e_k, e_\ell]$, où $1 \leq i \neq j \neq k \neq \ell \leq 4$. Elle échange e_k et e_ℓ tout en fixant e_i et e_j . Comme $\mathcal{Ext}(\Delta_3)$ compte exactement quatre éléments,

$$\mathfrak{S}(\mathcal{Ext}(\Delta_3)) = \mathfrak{S}_4,$$

ainsi l'isométrie s , définie par

$$s : \begin{cases} e_k \mapsto e_\ell \\ e_\ell \mapsto e_k \\ e_i \mapsto e_i \\ e_j \mapsto e_j \end{cases}$$

correspond exactement à la transposition $(e_k \ e_\ell)$ de $\mathfrak{S}(\mathcal{Ext}(\Delta_3))$, et donc à $(k \ \ell) \in \mathfrak{S}_4$. On a ainsi $\varphi(s) = \sigma_s = (k \ \ell)$, c'est-à-dire :

$$\forall (i \ j) \in \mathfrak{S}_4, \exists s \in \text{Isom}(\Delta_3), (i \ j) = \varphi(s).$$

Passons au cas général : soit $\sigma \in \mathfrak{S}_4$. Comme $\mathfrak{T}_4$ engendre $\mathfrak{S}_4$, il existe un entier $k \geq 1$ et $(\tau_1, \dots, \tau_k) \in \mathfrak{T}_4^k$ tels que

$$\sigma = \tau_1 \circ \dots \circ \tau_k.$$

Par le paragraphe précédent,

$$\forall i \in \{1, \dots, k\}, \exists s_i \in \text{Isom}(\Delta_3), \tau_i = \varphi(s_i)$$

et ainsi

$$\sigma = \varphi(s_1) \circ \dots \circ \varphi(s_k).$$

et comme φ est un morphisme,

$$\sigma = \varphi(s_1 \circ \dots \circ s_k).$$

En posant $i = s_1 \circ \dots \circ s_k \in \text{Isom}(\Delta_3)$, on obtient

$$\forall \sigma \in \mathfrak{S}_4, \exists i \in \text{Isom}(\Delta_3), \sigma = \varphi(i),$$

ce qui prouve la surjectivité de φ .

Injectivité :

Soit $f \in \ker \varphi$: alors $\varphi(f) = \sigma_f = \text{id}$, ce qui signifie que

$$\forall i \in \{1, \dots, 4\}, \sigma_f(i) = i,$$

et donc que

$$\forall i \in \{1, \dots, 4\}, f(e_i) = e_i.$$

En tant qu'endomorphisme de $\mathbb{R}^4$, f est entièrement déterminée par l'image d'une base. Coïncidant avec id sur la base canonique B de $\mathbb{R}^4$, elle lui est donc égale, si bien que

$$\ker \varphi = \{\text{id}\}.$$

Le morphisme φ est donc injectif. □

Corollaire 1.24.

Les groupes $\text{Isom}(\Delta_3)$ et $\mathfrak{S}_4$ sont isomorphes.

1.3.2 Étude géométrique

Examinons en détail les types possibles dans $\mathfrak{S}_4$. La remarque 1.19 ramène cette question à l'énumération des partitions de l'entier 4 :

$$4 = 1 + 1 + 1 + 1$$

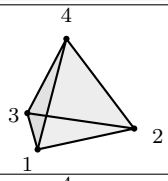
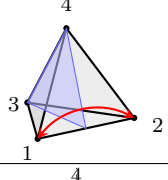
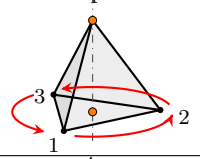
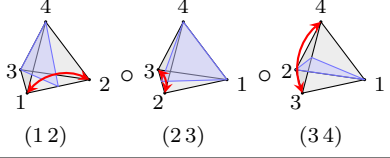
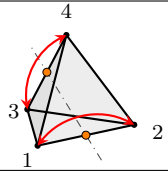
$$4 = 2 + 1 + 1$$

$$4 = 3 + 1$$

$$4 = 4$$

$$4 = 2 + 2.$$

Il existe donc cinq types de permutations. Le tableau suivant les récapitule, avec leur signature et leur interprétation géométrique comme isométrie du tétraèdre.

Type	Exemple dans $\mathfrak{S}_4$	Isométrie du tétraèdre associée	Signature ε
(1,1,1,1)	id		1
(2,1,1)	(1 2)(3)(4)		-1
(3,1)	(1 2 3)(4)		$(-1)^{3-1} = 1$
(4)	(1 2 3 4) = (12)(23)(34)		$(-1)^{4-1} = -1$
(2,2)	(1 2)(3 4)		$(-1)(-1) = 1$

Ce tableau met en évidence deux catégories d'isométries : celles qui sont réalisables dans notre espace tridimensionnel et celles qui ne le sont pas. En effet, réaliser la symétrie associée à une transposition obligerait le tétraèdre à se traverser lui-même ; de même, un 4-cycle reviendrait à enchaîner trois symétries consécutives, et donc à ce que le solide se traverse trois fois de suite. Nous qualifions ces isométries de non réalisables.

Le lecteur attentif aura remarqué que ces permutations ont pour signature -1 , alors que les isométries réalisables (l'identité, la rotation autour d'un axe passant par un sommet et le centre de gravité du solide, et la rotation autour d'un axe passant par les milieux de deux arêtes opposées) ont une signature égale à 1.

Ainsi, la signature (dans le cadre du groupe symétrique) ou, de manière équivalente, le déterminant (en algèbre linéaire) indiquent si la transformation de l'espace représentée par une permutation/un endomorphisme, force l'espace à se traverser lui-même : une valeur négative signale précisément ce phénomène.

En définitive, $\mathcal{A}_4$ s'identifie au sous-groupe de $\mathfrak{S}_4$ qui contient les isométries réalisables du tétraèdre. Ce point de vue géométrique éclaire bien mieux la structure de groupe de cet ensemble qu'une simple vérification des axiomes ne le ferait.

1.4 Le cas général : le simplexe

Définition 1.25. Soit $B = (e_1, \dots, e_{n+1})$ la base canonique de $\mathbb{R}^{n+1}$. On définit le simplexe régulier de taille n , noté Δ_n , comme l'enveloppe convexe de B .

Nous pouvons à présent généraliser le théorème 1.23 à un n quelconque :

Théorème 1.26.

On considère le morphisme

$$\begin{array}{ccc} \varphi : (\text{Isom}(\Delta_n), \circ) & \longrightarrow & (\mathfrak{S}_{n+1}, \circ) \\ f & \longmapsto & \sigma_f \end{array},$$

où pour tout $1 \leq i \leq n+1$, $\sigma_f(i) = j$ avec j vérifiant $f(e_i) = e_j$.

Le morphisme φ est bijectif.

Démonstration.

La preuve suit de près celle du cas $n = 3$: nous n'en détaillons donc que les points qui diffèrent.

Surjectivité :

Comme en dimension 3, on a

$$\text{Isom}(\Delta_n) \curvearrowright \mathcal{Ext}(\Delta_n),$$

de sorte qu'une isométrie de Δ_n est entièrement déterminée par son action sur les seuls points extrémaux.

Considérons alors la symétrie $s \in \text{Isom}(\Delta_n)$ par rapport à l'hyperplan contenant $e_{i_1}, \dots, e_{i_{n-1}}$ et le milieu de $[e_{i_n}, e_{i_{n+1}}]$, où $1 \leq i_1 \neq \dots \neq i_{n+1} \leq n+1$. Elle échange e_{i_n} et $e_{i_{n+1}}$ tout en fixant les $n-1$ points restants.

Par le même argument qu'en dimension 3, s correspond exactement à la transposition $(e_{i_n} \ e_{i_{n+1}})$ de $\mathfrak{S}(\mathcal{Ext}(\Delta_n))$, donc à $(i_n \ i_{n+1}) \in \mathfrak{S}_{n+1}$.

Toute transposition de $\mathfrak{S}_{n+1}$ est ainsi l'image par φ d'un élément de $\text{Isom}(\Delta_n)$. Comme $\mathfrak{T}_{n+1}$ engendre $\mathfrak{S}_{n+1}$ et que φ est un morphisme, la surjectivité de φ s'ensuit.

Injectivité :

Comme en dimension 3, tout $f \in \ker \varphi$ fixe la base B de $\mathbb{R}^{n+1}$. Coïncidant avec id sur B , sa linéarité entraîne alors que

$$f = \text{id}.$$

Ainsi $\ker \varphi = \{\text{id}\}$, et φ est injectif.

Le morphisme φ est donc bien bijectif. □

Comme précédemment, on en déduit le corollaire suivant :

Corollaire 1.27.

Les groupes $\text{Isom}(\Delta_n)$ et $\mathfrak{S}_{n+1}$ sont isomorphes.

Nous pouvons enfin conclure cette partie par le résultat tant attendu :

Théorème 1.28.

Le groupe symétrique $\mathfrak{S}_{n+1}$ agit sur le simplexe Δ_n .

Démonstration.

Par construction, $\text{Isom}(\Delta_n) \curvearrowright \Delta_n$. Or, le corollaire 1.27 assure que les groupes $\mathfrak{S}_{n+1}$ et $\text{Isom}(\Delta_n)$ sont isomorphes, c'est-à-dire qu'ils se comportent de la même manière. Il est dès lors naturel d'écrire

$$\boxed{\mathfrak{S}_{n+1} \curvearrowright \Delta_n}.$$

□

Chapitre 2

Simplicité de $\mathcal{A}_n$

2.1 SimPLICITÉ d'un groupe

Définition 2.1. Soit G un groupe et $H < G$. On dit que H est distingué dans G , et l'on note $H \triangleleft G$, si

$$\forall h \in H, \forall g \in G, ghg^{-1} \in H.$$

Autrement dit, H est stable par conjugaison par tout élément de G .

Définition 2.2. Soit G un groupe et e son élément neutre. G est dit simple si ses seuls sous-groupes distingués sont lui-même et $\{e\}$.

Remarque 2.3. Un groupe abélien G possédant au moins un sous-groupe non trivial ne peut être simple. En effet, pour tout sous-groupe non trivial $H < G$, on a

$$\forall h \in H, \forall g \in G, ghg^{-1} = gg^{-1}h = h \in H.$$

Tout sous-groupe non trivial H de G est donc distingué dans G , ce qui contrevient à la simplicité.

Ces hypothèses — un groupe abélien possédant des sous-groupes non triviaux — excluent d'emblée la simplicité, mais elles restent très fortes. Cherchons plutôt un critère plus fin, fondé sur le centre d'un groupe, c'est-à-dire l'ensemble des éléments qui commutent avec tous les autres.

Définition 2.4. Soit G un groupe. On appelle centre de G , que l'on note $Z(G)$, l'ensemble

$$Z(G) = \{h \in G \mid \forall g \in G, gh = hg\}.$$

Remarquons d'abord que l'élément neutre e de G appartient toujours à son centre, puisque

$$\forall g \in G, ge = eg.$$

Mais une propriété bien plus intéressante se dégage :

Propriété 2.5.

Soit G un groupe, alors $Z(G)$ est un sous-groupe de G .

Démonstration.

Nous avons déjà vu que le neutre appartient à $Z(G)$, cet ensemble est donc non vide.

Soient $h, h_1 \in Z(G)$ et $g \in G$. Alors :

- puisque $hg = gh$, on a $g = h^{-1}gh$ puis $gh^{-1} = h^{-1}g$, donc $h^{-1} \in Z(G)$. Ceci assure la stabilité par inverse de $Z(G)$.
- en utilisant l'associativité de la loi de G , $hh_1g = h(h_1g) = hgh_1 = (hg)h_1 = gh h_1$, donc $hh_1 \in Z(G)$. Ceci garantit la stabilité par produit de $Z(G)$.

Ainsi $Z(G)$ est bien un sous-groupe de G : $Z(G) < G$. □

Nous en tirons enfin un critère de non-simplicité :

Proposition 2.6.

Soit G un groupe de neutre e . Son centre $Z(G)$ est toujours distingué dans G . En particulier, s'il n'est pas trivial, alors G est non-simple.

Démonstration.

Montrons d'abord que $Z(G)$ est distingué dans G .

Pour $g \in G$ et $h \in Z(G)$, on a $ghg^{-1} = (gh)g^{-1} = hgg^{-1} = h \in Z(G)$, d'où le caractère distingué de $Z(G)$ dans G . Deux cas se présentent alors :

- Si $Z(G) = G$, G est abélien, ce qui est absurde au vu des hypothèses.
- Sinon, $Z(G)$ est un sous-groupe strict de G , non réduit à $\{e\}$. G possède ainsi un sous-groupe distingué non trivial : il est non simple. □

2.2 Les cas $n = 1, 2$ et 3

Explicitons les groupes symétriques de tailles 1, 2 et 3 :

$$\begin{aligned}\mathfrak{S}_1 &= \{\text{id}\} \\ \mathfrak{S}_2 &= \{\text{id}, (1\ 2)\} \\ \mathfrak{S}_3 &= \{\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}\end{aligned}$$

ainsi que les groupes alternés associés :

$$\begin{aligned}\mathcal{A}_1 &= \mathcal{A}_2 = \{\text{id}\} \\ \mathcal{A}_3 &= \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}.\end{aligned}$$

Les groupes $\mathcal{A}_1$ et $\mathcal{A}_2$ n'ont manifestement aucun sous-groupe non trivial : ils sont donc simples. Pour conclure sur $\mathcal{A}_3$, introduisons le théorème suivant :

Théorème 2.7 (de Lagrange).

Soit G un groupe fini. Soit $H < G$, on a $|H| \mid |G|$. Plus précisément,

$$|G| = |H| \times [H : G] = |H| \times |G/H|.$$

où $[H : G]$ représente l'indice de H dans G , soit (dans le cas fini) le nombre de classes d'équivalence dans G pour la relation : $xRy \iff x^{-1}y \in H$. On retrouve ceci dans la seconde égalité avec $|G/H|$, qui correspond exactement au cardinal de l'ensemble des classes d'équivalence pour cette relation.

Soit H un sous-groupe de $\mathcal{A}_3$: alors $|H| \mid |\mathcal{A}_3| = 3$, si bien que H est d'ordre 1 ou 3. Ainsi $H = \{\text{id}\}$ ou $H = \mathcal{A}_3$: le groupe $\mathcal{A}_3$ n'a aucun sous-groupe non trivial, il est donc simple.

2.3 Le cas $n = 4$: l'exception**2.3.1 Non-simplicité de $\mathcal{A}_4$**

Le groupe alterné de taille 4 est le seul à ne pas être simple. Pour l'établir, nous allons exhiber un sous-groupe distingué dans $\mathcal{A}_4$.

Explicitons d'abord $\mathcal{A}_4$, comme nous l'avons fait plus haut :

$$\begin{aligned} \mathcal{A}_4 = & \{\text{id}, \\ & (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \\ & (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \end{aligned}$$

Il réunit l'identité, les huit 3-cycles et les trois doubles transpositions de $\mathfrak{S}_4$.

Le théorème 2.7 permet de resserrer la recherche : comme $|\mathcal{A}_4| = 12$, un éventuel sous-groupe a pour cardinal 1, 2, 3, 4, 6 ou 12.

On pose alors

$$\mathcal{V}_4 = \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Intuitivement, $\mathcal{V}_4$ devrait bien former un sous-groupe, puisqu'il rassemble l'identité et toutes les doubles transpositions.

Propriété 2.8.

L'ensemble $\mathcal{V}_4$ est un sous-groupe de $\mathcal{A}_4$.

Démonstration.

Par définition, $\text{id} \in \mathcal{V}_4$, cet ensemble est donc non vide.

Posons $\tau_1 = (1\ 2)(3\ 4)$, $\tau_2 = (1\ 3)(2\ 4)$ et $\tau_3 = (1\ 4)(2\ 3)$. La composition fournit les relations

$$\tau_1 \circ \tau_2 = (1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3) = \tau_3$$

et de même

$$\tau_2 \circ \tau_3 = \tau_1$$

$$\tau_3 \circ \tau_1 = \tau_2$$

ce qui garantit la stabilité de $\mathcal{V}_4$ par composition.

Par ailleurs, pour tout $i \in \{1, 2, 3\}$,

$$\tau_i^2 = (p \ q)(r \ s)(p \ q)(r \ s) = (p \ q)^2(r \ s)^2 = \text{id}^2 = \text{id},$$

les τ_i sont donc des involutions, et $\mathcal{V}_4$ est stable par passage à l'inverse.

Ainsi $\boxed{\mathcal{V}_4 < \mathcal{A}_4}$.

□

Reste à savoir si $\mathcal{V}_4$ est distingué dans $\mathcal{A}_4$: c'est bien le cas.

Propriété 2.9.

Le sous-groupe $\mathcal{V}_4$ est distingué dans $\mathcal{A}_4$.

Démonstration.

Soient $g \in \mathcal{A}_4$ et $h \in \mathcal{V}_4$.

- Si $h = \text{id}$, alors $ghg^{-1} = gg^{-1} = \text{id} \in \mathcal{V}_4$.
- Sinon, $h = (i \ j)(k \ \ell)$, et

$$ghg^{-1} = g(i \ j)(k \ \ell)g^{-1} = g(i \ j)g^{-1}g(k \ \ell)g^{-1}.$$

Or, pour toute transposition $\tau = (p \ q) \in \mathfrak{S}_4$ et $g = \begin{pmatrix} p & q & r & s \\ g(p) & g(q) & g(r) & g(s) \end{pmatrix}$,

$$g\tau g^{-1} = \begin{pmatrix} p & q & r & s \\ g(p) & g(q) & g(r) & g(s) \end{pmatrix} (p \ q) \begin{pmatrix} g(p) & g(q) & g(r) & g(s) \\ p & q & r & s \end{pmatrix} = (g(p) \ g(q)).$$

Ainsi

$$ghg^{-1} = (g(i) \ g(j))(g(k) \ g(\ell)).$$

Comme $i \neq j \neq k \neq \ell$ et que g est une permutation de $\{1, \dots, 4\}$, on a $g(i) \neq \dots \neq g(\ell)$. Dès lors $ghg^{-1} = (g(i) \ g(j))(g(k) \ g(\ell))$ est une double transposition, donc un élément de $\mathcal{V}_4$.

La conjugaison par un élément de $\mathcal{A}_4$ laisse donc $\mathcal{V}_4$ stable, ce qui prouve que $\boxed{\mathcal{V}_4 \triangleleft \mathcal{A}_4}$. □

Nous obtenons enfin la propriété de $\mathcal{A}_4$ que nous cherchions :

Proposition 2.10.

$\mathcal{A}_4$ est non-simple.

Démonstration.

Le sous-groupe $\mathcal{V}_4$ est distingué dans $\mathcal{A}_4$ sans être réduit au neutre ni égal à $\mathcal{A}_4$ tout entier : $\mathcal{A}_4$ est donc non-simple. □

2.3.2 Complément : le groupe de Klein

Cette partie met en lumière le lien profond entre $\mathcal{V}_4$ et le groupe de Klein.

Définition 2.11. On appelle groupe de Klein le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. Il comporte quatre éléments que l'on peut expliciter :

$$\text{id} = (0, 0), \quad k_1 = (1, 0), \quad k_2 = (0, 1), \quad k_3 = (1, 1).$$

Observons l'effet de quelques opérations dans ce groupe :

$$\begin{aligned} k_1 + k_1 &= (2, 0) = (0, 0) = \text{id} \\ k_2 + k_2 &= (0, 2) = (0, 0) = \text{id} \\ k_3 + k_3 &= (2, 2) = (0, 0) = \text{id} \\ k_1 + k_2 &= (1, 1) = (1, 1) = k_3 \\ k_2 + k_3 &= (1, 2) = (1, 0) = k_1 \\ k_3 + k_1 &= (2, 1) = (0, 1) = k_2 \end{aligned}$$

Les éléments k_1, k_2 et k_3 sont donc tous d'ordre 2, et la somme de deux d'entre eux distincts donne le troisième... c'est exactement le comportement du groupe $\mathcal{V}_4$ (voir la propriété 2.8). En ce sens, le groupe de Klein et $\mathcal{V}_4$ sont isomorphes. $\mathcal{V}_4$ est simplement une autre représentation visuelle de ce groupe incontournable.

2.4 Le cas $n = 5$

2.4.1 Corps finis

Dans toute cette section, q désigne un entier naturel non nul.

Notation 2.12. On note $\mathbb{F}_q$ le corps fini à q éléments.

L'entier q doit toutefois remplir certaines conditions pour que $\mathbb{F}_q$ existe ; nous les détaillons ci-dessous.

Notation 2.13. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Proposition 2.14.

Soit $p \in \mathcal{P}$. Si $q = p$, alors $\mathbb{F}_q$ existe et

$$\mathbb{F}_q = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

Démonstration.

Soit $\mathbb{K}$ un corps quelconque ayant p éléments, de neutre multiplicatif $1_{\mathbb{K}}$ et de neutre additif $0_{\mathbb{K}}$. En additionnant successivement $1_{\mathbb{K}}$ à lui-même, on forme l'ensemble :

$$S = \{0_{\mathbb{K}}, 1_{\mathbb{K}}, 1_{\mathbb{K}} + 1_{\mathbb{K}}, 1_{\mathbb{K}} + 1_{\mathbb{K}} + 1_{\mathbb{K}}, \dots\}$$

Ainsi, l'ensemble S est un sous-groupe du groupe additif $(\mathbb{K}, +)$. Par le théorème de Lagrange, $|S| \mid |\mathbb{K}| = p \in \mathcal{P}$. De plus, nous savons que S contient au moins deux éléments

distincts : $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$, ainsi $|S| = p = |\mathbb{K}|$ et $S \subseteq \mathbb{K}$, d'où $S = \mathbb{K}$. Finalement, $1_{\mathbb{K}}$ est donc générateur de $(\mathbb{K}, +)$, ce qui en fait un groupe cyclique de cardinal p . Dès lors, on a nécessairement

$$\boxed{\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}}$$

□

Il n'existe qu'un seul autre cas où le corps à q éléments existe.

Proposition 2.15.

Soit $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n . Si $q = p^n$, alors $\mathbb{F}_q$ existe et

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P).$$

Démonstration.

Nous admettons ici que tout corps fini de cardinal $q = p^n$ se réalise **uniquement** comme quotient de l'anneau des polynômes d'indéterminée X et à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ par l'idéal engendré par un polynôme P irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et de degré n . En revanche, nous montrons que ce procédé constructif aboutit bien à un corps à $q = p^n$ éléments. Montrons que $\mathbb{F}_p[X]/(P)$ est bien un corps :

Soit $\bar{Q} \in \mathbb{F}_p[X]/(P)$, $\bar{Q} \neq \bar{0}$. On note Q un représentant de la classe $\bar{Q}$. Par irréductibilité de P , P et Q sont premiers entre eux et on applique alors le lemme de Bézout :

$$\exists (U, V) \in \mathbb{F}_p[X]^2, \quad PU + QV = 1$$

En passant aux classes on obtient :

$$\begin{aligned} \overline{PU + QV} &= \bar{1} \\ \implies \overline{PU} + \overline{QV} &= \bar{1} \\ \implies \bar{P}\bar{U} + \bar{Q}\bar{V} &= \bar{1} \\ \implies \bar{Q}\bar{V} &= \bar{1} \text{ car } \bar{P} = \bar{0} \end{aligned}$$

Ainsi, nous avons trouvé un inverse multiplicatif $\bar{V}$ à $\bar{Q}$ dans $\mathbb{F}_p[X]/(P)$. Finalement, tout élément non nul de $\mathbb{F}_p[X]/(P)$ est donc inversible, ce qui en fait un corps. Dénombrons-le. Plus concrètement, en tant qu'ensemble de restes lors de la division euclidienne par P , on a :

$$\mathbb{F}_p[X]/(P) = \{ a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_1X + a_0 \mid (a_0, a_1, \dots, a_{n-2}, a_{n-1}) \in \mathbb{F}_p^n \}$$

Ainsi, il y a p choix pour a_0 , puis p choix pour a_1 , puis p choix pour a_2 , ..., et enfin p choix pour a_{n-1} . Finalement, cet ensemble contient bien $p^n = q$ éléments, soit

$$\boxed{|\mathbb{F}_p[X]/(P)| = p^n = q}.$$

□

Remarque 2.16. Une question naturelle qui émerge de cette construction : “est-ce que le polynôme P par lequel on quotiente a une importance ?”. Lors de la preuve, on observe que

seuls le degré et l'irréductibilité de P sont déterminants, et aucunement ses coefficients. En effet, du point de vue de la structure algébrique, on peut montrer de manière analogue que le corps $\mathbb{F}_q$ construit a toujours une structure de $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel. Quel que soit le polynôme P par lequel on quotiente (du moment qu'il est de degré n et irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$), on obtiendra un corps fini à $q = p^n$ éléments. On notera que dans la pratique, un choix astucieux du polynôme P est judicieux, afin de simplifier les divisions euclidiennes de polynômes à effectuer. En somme, le choix de P importe, mais pas trop.

2.4.2 Caractère isomorphe de $\mathrm{SL}_2(\mathbb{F}_4)$ et $\mathcal{A}_5$

Pour établir la simplicité de $\mathcal{A}_5$, nous cherchons un groupe qui lui est isomorphe et plus commode à étudier. Un groupe de matrices s'impose naturellement, leur classification étant bien maîtrisée grâce à la réduction de Jordan. La propriété suivante servira de point de départ à cette recherche. Dans la suite, n désigne un entier naturel et $\mathbb{K}$ un corps.

Action naturelle de $\mathrm{GL}_n(\mathbb{K})$ et fidélité

Propriété 2.17.

Le groupe linéaire $\mathrm{GL}_n(\mathbb{K})$ agit naturellement sur $\mathbb{K}^n$.

Introduisons à présent un ensemble crucial pour la suite.

Définition 2.18. On définit l'espace projectif de l'espace vectoriel $\mathbb{K}^n$ par

$$\mathbb{P}^{n-1}(\mathbb{K}) = \{\mathrm{Vect}(X) \mid X \in \mathbb{K}^n, X \neq 0\}.$$

Il correspond à l'ensemble des droites vectorielles de $\mathbb{K}^n$.

On peut alors affiner l'action du groupe linéaire : elle se restreint en fait à l'espace projectif associé au corps de base.

Propriété 2.19.

L'application

$$\begin{aligned} \varphi : \mathrm{GL}_n(\mathbb{K}) \times \mathbb{P}^{n-1}(\mathbb{K}) &\longrightarrow \mathbb{P}^{n-1}(\mathbb{K}) \\ (M, d) &\longmapsto M \cdot d = Md \end{aligned}$$

est une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathbb{P}^{n-1}(\mathbb{K})$.

Démonstration.

On vérifie les axiomes de la définition 1.22. Soit $d \in \mathbb{P}^{n-1}(\mathbb{K})$, alors il existe $X \in \mathbb{K}^n$ tel que $d = \mathrm{Vect}(X)$. On a alors :

- i) $\varphi(I_n, d) = I_n \mathrm{Vect}(X) = \mathrm{Vect}(I_n X) = \mathrm{Vect}(X) = d$.
- ii) Soient $M, N \in \mathrm{GL}_n(\mathbb{K})$, alors

$$M \cdot (N \cdot d) = M \cdot (N \mathrm{Vect}(X)) = M \cdot \mathrm{Vect}(NX) = \mathrm{Vect}(MNX) = (MN) \cdot d.$$

□

Pour la suite, on considérera plutôt le morphisme

$$\begin{aligned}\phi : \text{GL}_n(\mathbb{K}) &\longrightarrow \mathfrak{S}(\mathbb{P}^{n-1}(\mathbb{K})) \\ M &\longmapsto \phi(M)\end{aligned}$$

qui vérifie $\forall M \in \text{GL}_n(\mathbb{K}), \forall d \in \mathbb{P}^{n-1}(\mathbb{K}), \phi(M)(d) = \varphi(M, d)$.

Cette action est loin d'être fidèle : par exemple, dilater ou contracter une droite par une homothétie de rapport λ la laisse inchangée. Cherchons donc à identifier le noyau de l'action.

Lemme 2.20.

Le noyau de ϕ est l'ensemble des homothéties de $\mathcal{M}_n(\mathbb{K})$. Autrement dit,

$$\ker \phi = \{\lambda I_n, \lambda \in \mathbb{K}^*\}.$$

Démonstration.

On note $H = \{\lambda I_n, \lambda \in \mathbb{K}^*\}$ et l'on procède par double inclusion.

Soit $M \in H$, ainsi il existe $\lambda \in \mathbb{K}^*$ tel que $M = \lambda I_n$. Soit $d \in \mathbb{P}^{n-1}(\mathbb{K})$, et l'on note $d = \text{Vect}(X)$ avec $X \in \mathbb{K}^n$, il vient :

$$\phi(M)(d) = \varphi(M, d) = Md = \lambda I_n \text{Vect}(X) = \text{Vect}(\lambda I_n X) = \text{Vect}(X) = d$$

Ainsi, pour tout $d \in \mathbb{P}^{n-1}(\mathbb{K})$, $\phi(M)(d) = d$, d'où $\phi(M) = \text{id}_{\mathbb{P}^{n-1}(\mathbb{K})}$ et $M \in \ker \phi$.

Finalement, $\boxed{H \subset \ker \phi}$.

Réciproquement, soit $M \in \ker \phi$. Ainsi, pour tout $d \in \mathbb{P}^{n-1}(\mathbb{K})$, $\phi(M)(d) = d$, i.e. $\boxed{Md = d}$ $(\star)$. On singularise alors une droite vectorielle d quelconque en posant $d = \text{Vect}(X)$ avec $X \in \mathbb{K}^n$. Ainsi, $(\star)$ donne $M \text{Vect}(X) = \text{Vect}(X)$, soit $\text{Vect}(MX) = \text{Vect}(X)$, et il vient alors :

$$MX \in \text{Vect}(MX) = \text{Vect}(X) \implies \exists \lambda_X \in \mathbb{K}^*, MX = \lambda_X X$$

Ce résultat étant établi pour une droite vectorielle d quelconque et donc pour un vecteur directeur X quelconque, on obtient :

$$\boxed{\forall X \in \mathbb{K}^n, \exists \lambda_X \in \mathbb{K}^*, MX = \lambda_X X} \quad (\star\star)$$

ce qui permet alors de montrer que M est une homothétie.

On note $B = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$ et u l'endomorphisme canoniquement associé à M .

D'une part, par $(\star\star)$, pour tout $i \in \{1, \dots, n\}$, il existe $\lambda_i \in \mathbb{K}^*$ tel que $u(e_i) = \lambda_i e_i$. D'autre part, par $(\star\star)$ à nouveau, il existe $\lambda \in \mathbb{K}^*$ tel que :

$$u\left(\sum_{i=1}^n e_i\right) = \lambda \sum_{i=1}^n e_i$$

La linéarité de u donne alors :

$$\sum_{i=1}^n \lambda e_i = \lambda \sum_{i=1}^n e_i = u\left(\sum_{i=1}^n e_i\right) = \sum_{i=1}^n u(e_i) = \sum_{i=1}^n \lambda_i e_i \implies \forall i \in \{1, \dots, n\}, \lambda_i = \lambda$$

par unicité de la décomposition de tout vecteur dans la base B . Finalement, pour tout $i \in \{1, \dots, n\}$, $u(e_i) = \lambda e_i$, et u coïncide donc avec $\lambda \text{id}_{\mathbb{K}^n}$ sur la base B . Par linéarité de u , on conclut finalement $u = \lambda \text{id}_{\mathbb{K}^n}$ et donc $M = \lambda I_n$; d'où $M \in H$ et $\ker \phi \subset H$

Par double inclusion, $\ker \phi = H = \{\lambda I_n, \lambda \in \mathbb{K}^*\}$ □

Pour poursuivre, nous avons besoin d'un résultat important sur le noyau d'un morphisme de groupes.

Propriété 2.21.

Soit G un groupe et $H < G$. H est distingué dans G si et seulement s'il existe F un groupe tel que H soit le noyau d'un morphisme de groupes de G vers F .

Démonstration.

On raisonne par double implication.

$\Leftarrow$ Supposons d'abord qu'il existe F un groupe tel que $H = \ker \varphi$, où φ est un morphisme de groupes de G vers F . Soit $h \in H$, soit $g \in G$, on obtient :

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) \text{ car } h \in \ker \varphi$$

Or, $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_F$. Ainsi, $\varphi(ghg^{-1}) = e_F$ et $ghg^{-1} \in \ker \varphi = H$. Finalement, pour tous $g \in G, h \in H$, $ghg^{-1} \in H$, et $H \triangleleft G$.

$\Rightarrow$ Réciproquement, on suppose $H \triangleleft G$. On pose alors $F = G/H$, qui a bien une structure de groupe car H est distingué dans G , et :

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

le morphisme de projection canonique. De plus,

$$g \in \ker \pi \iff \pi(g) = e_{G/H} \iff gH = H \iff g \in H$$

ce qui assure $H = \ker \pi$ □

Nous pouvons maintenant considérer le quotient suivant.

Définition 2.22. On définit le groupe linéaire projectif comme

$$\text{PGL}_n(\mathbb{K}) = \text{GL}_n(\mathbb{K}) / \ker \phi.$$

En effet, de par la propriété 2.21, $\ker \phi \triangleleft \text{GL}_n(\mathbb{K})$, et cet ensemble quotient a donc bien une structure de groupe.

On obtient alors que le morphisme

$$\begin{aligned} \psi : \mathrm{PGL}_n(\mathbb{K}) &\longrightarrow \mathfrak{S}(\mathbb{P}^{n-1}(\mathbb{K})) \\ \bar{M} &\longmapsto \psi(\bar{M}) \end{aligned}$$

est injectif : autrement dit, l'action associée est dorénavant fidèle.

Corps à quatre éléments

Construisons maintenant le corps à quatre éléments, qui jouera un rôle central dans la suite.

Plaçons-nous dans $\mathbb{F}_2[X]$. On vérifie aisément que le seul polynôme irréductible de degré 2 dans cet anneau est $X^2 + X + 1$. La proposition 2.15 fournit alors le corps à quatre éléments :

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \omega, \omega^2\}$$

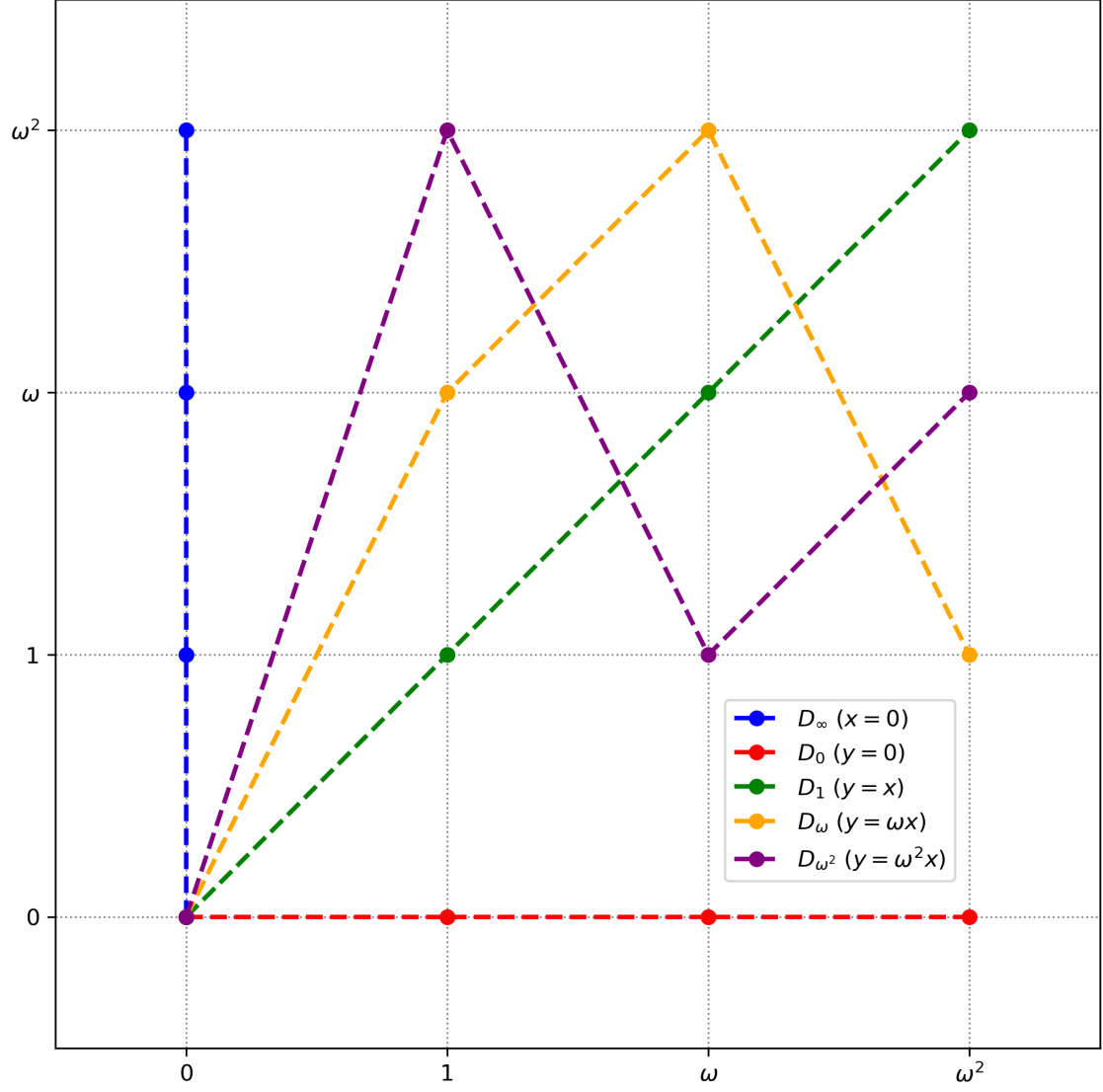
où ω est défini par la relation $\omega^2 + \omega + 1 = 0$, soit $\omega^2 = \omega + 1$.

Nous pouvons alors dresser les tables d'addition et de multiplication de $\mathbb{F}_4$, en gardant à l'esprit que l'on travaille en caractéristique 2, le corps de base étant $\mathbb{Z}/2\mathbb{Z}$.

+	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	0	ω^2	ω
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\times$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

Maintenant que le comportement de $\mathbb{F}_4$ est connu, intéressons-nous à l'ensemble de ses droites vectorielles : $\mathbb{P}^1(\mathbb{F}_4)$, composé des éléments suivants :



Ces droites sont au nombre de cinq, d'où

$$\mathfrak{S}(\mathbb{P}^1(\mathbb{F}_4)) = \mathfrak{S}_5.$$

Dans le cas $n = 2$, ce qui précède se réécrit alors par : le morphisme

$$\begin{aligned} \psi : \text{PGL}_2(\mathbb{F}_4) &\longrightarrow \mathfrak{S}_5 \\ \bar{M} &\longmapsto \psi(\bar{M}) \end{aligned}$$

est injectif.

Isomorphisme entre $\text{SL}_2(\mathbb{F}_4)$ et $\mathcal{A}_5$

Il reste à simplifier l'espace de départ, peu maniable et intuitif en tant que groupe de classes d'équivalence. $\text{SL}_2(\mathbb{F}_4)$ apparaît comme un bon candidat : c'est un sous-groupe de $\text{GL}_2(\mathbb{F}_4)$, et sa condition d'existence basée sur le déterminant se fonde dans un contexte de dilatation ou de contraction de droites. On peut aussi remarquer, comme souligné plus

haut, que le déterminant est aux matrices ce que la signature est aux permutations. Le groupe alterné étant le noyau de la signature, il vient naturellement à l'idée d'étudier son homologue, le noyau du déterminant.

On considère donc le morphisme

$$\begin{aligned}\phi_{\text{SL}} : \text{SL}_2(\mathbb{F}_4) &\longrightarrow \mathfrak{S}_5 \\ M &\longmapsto \phi_{\text{SL}}(M)\end{aligned}$$

associé à l'action de $\text{SL}_2(\mathbb{F}_4)$ sur $\mathbb{P}^1(\mathbb{F}_4)$.

Définition 2.23. On définit le groupe spécial linéaire projectif en dimension 2 sur le corps $\mathbb{F}_4$ comme

$$\text{PSL}_2(\mathbb{F}_4) = \text{SL}_2(\mathbb{F}_4) / \ker \phi_{\text{SL}}.$$

En tant que noyau, de par la propriété 2.21, $\ker \phi_{\text{SL}}$ est bien distingué dans $\text{SL}_2(\mathbb{F}_4)$, ce qui assure une structure de groupe au quotient.

Il s'avère alors que $\ker \phi_{\text{SL}}$ contient très peu d'éléments, un seul en réalité, ce qui est naturel au vu de la structure de $\text{SL}_2(\mathbb{F}_4)$.

Propriété 2.24.

Les groupes $\text{PSL}_2(\mathbb{F}_4)$ et $\text{SL}_2(\mathbb{F}_4)$ sont égaux.

Démonstration.

En se référant à la définition 2.23 de $\text{PSL}_2(\mathbb{F}_4)$, il suffit de montrer que

$$\ker \phi_{\text{SL}} = \{I_2\}.$$

Soit $M \in \ker \phi_{\text{SL}}$, puisque $\text{SL}_2(\mathbb{F}_4) \subset \text{GL}_2(\mathbb{F}_4)$ le lemme 2.20 s'applique et l'on obtient

$$\exists \lambda \in \mathbb{F}_4^*, M = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

De plus, $M \in \text{SL}_2(\mathbb{F}_4)$ donc $\det(M) = 1 = \lambda^2$. Cela nous conduit à résoudre $\lambda^2 - 1 = 0$, ce qui donne

$$\begin{aligned}\lambda^2 - 1 &= 0 \\ \implies (\lambda + 1)(\lambda - 1) &= 0 \\ \implies (\lambda - 1)^2 &= 0 \\ \implies \lambda &= 1\end{aligned}$$

Ainsi $M = I_2$ et $\ker \phi_{\text{SL}} = \{I_2\}$, ce qui donne finalement :

$$\boxed{\text{PSL}_2(\mathbb{F}_4) = \text{SL}_2(\mathbb{F}_4)}.$$

□

Pour atteindre la simplification attendue, nous devons maintenant dénombrer les ensembles dont nous traitons.

Propriété 2.25.

Les groupes linéaire, linéaire projectif et spécial linéaire ont pour cardinal

$$|\mathrm{GL}_2(\mathbb{F}_4)| = 180 \quad \text{et} \quad |\mathrm{PGL}_2(\mathbb{F}_4)| = |\mathrm{SL}_2(\mathbb{F}_4)| = \frac{|\mathrm{GL}_2(\mathbb{F}_4)|}{3} = 60.$$

Démonstration.

Il est important de noter que l'on peut assimiler les colonnes d'une matrice inversible à des vecteurs constituant une base de l'espace ambiant. Ainsi, déterminer le nombre de bases du $\mathbb{F}_4$ -espace vectoriel $\mathbb{F}_4^2$ revient à dénombrer les matrices carrées inversibles de taille 2 à coefficients dans $\mathbb{F}_4$. Pour la première colonne, nous pouvons prendre n'importe quel vecteur non nul de $\mathbb{F}_4^2$: il y en a 15. Pour le second vecteur, il s'agit d'en choisir un non colinéaire au premier, il y a donc 12 choix. Ceci fait bien un total de $15 \times 12 = 180$ matrices.

Quant à $\mathrm{SL}_2(\mathbb{F}_4)$, à toute matrice M de déterminant 1 on peut associer trois matrices distinctes de $\mathrm{GL}_2(\mathbb{F}_4)$: elle-même, de déterminant 1 ; ωM , de déterminant ω^2 ; et $\omega^2 M$, de déterminant ω . D'où :

$$|\mathrm{GL}_2(\mathbb{F}_4)| = 3 |\mathrm{SL}_2(\mathbb{F}_4)| \implies |\mathrm{SL}_2(\mathbb{F}_4)| = \frac{|\mathrm{GL}_2(\mathbb{F}_4)|}{3} = \frac{180}{3} = 60$$

Pour conclure quant au cardinal de $\mathrm{PGL}_2(\mathbb{F}_4)$, il faut comprendre comment sont construites les classes d'équivalence qui le composent. Deux matrices P et Q dans la même classe $\bar{A} \in \mathrm{PGL}_2(\mathbb{F}_4)$ vérifient :

$$PRQ \iff P^{-1}Q \in \ker \psi = \{\lambda I_2, \lambda \in \mathbb{F}_4^*\} \implies Q = \lambda P, \lambda \in \mathbb{F}_4^*$$

La classe d'une matrice $M \in \mathrm{GL}_2(\mathbb{F}_4)$ donnée sera donc composée de M , ωM et $\omega^2 M$. Plus formellement, si on considère le morphisme

$$\tilde{\phi} : \mathrm{GL}_2(\mathbb{F}_4) \longrightarrow \mathfrak{S}_5,$$

défini à partir de ϕ (énoncé en dessous de la propriété 2.19) dans le cas $n = 2$ et $\mathbb{K} = \mathbb{F}_4$, son noyau est caractérisé par le lemme 2.20. Ainsi, $\ker \tilde{\phi} = \{\lambda I_2 \mid \lambda \in \mathbb{F}_4^*\} = \{I_2, \omega I_2, \omega^2 I_2\}$. On en déduit que $|\ker \tilde{\phi}| = 3$ et le théorème de Lagrange 2.7 nous permet de conclure :

$$|\mathrm{PGL}_2(\mathbb{F}_4)| = |\mathrm{GL}_2(\mathbb{F}_4) / \ker \tilde{\phi}| = \frac{|\mathrm{GL}_2(\mathbb{F}_4)|}{|\ker \tilde{\phi}|} = \frac{180}{3} = 60.$$

□

Armés de ces cardinaux, nous pouvons conclure quant à la simplification tant espérée.

Propriété 2.26.

Les groupes $\mathrm{PGL}_2(\mathbb{F}_4)$ et $\mathrm{SL}_2(\mathbb{F}_4)$ sont isomorphes.

Démonstration.

Il s'agit alors d'exhiber un isomorphisme entre $\mathrm{PGL}_2(\mathbb{F}_4)$ et $\mathrm{SL}_2(\mathbb{F}_4)$. Pour cela, nous allons commencer par montrer que tout élément de $\mathbb{F}_4$ est un carré.

- 0 et 1 sont leur propre carré.
- Puisque $\omega^3 = 1$, on obtient que $\omega = \omega^4 = (\omega^2)^2$.
- ω^2 est simplement le carré de ω .

Ainsi, pour tout $\lambda \in \mathbb{F}_4$, il existe $\mu \in \mathbb{F}_4$ tel que $\lambda = \mu^2$. Remarquons de plus que tout élément de $\mathbb{F}_4^*$ est d'ordre 3, l'égalité précédente devenant $\lambda^2 = \mu$ en élevant au carré.

On considère alors l'application

$$\varphi : \mathrm{PGL}_2(\mathbb{F}_4) \longrightarrow \mathrm{SL}_2(\mathbb{F}_4)$$

qui à une classe $\bar{M}$, dont on note M un représentant, associe $N = \frac{1}{\lambda_M} M$, où λ_M est défini par la relation $\lambda_M^2 = \det(M)$, soit $\lambda_M = \det(M)^2$. Vérifions que N est de déterminant 1 :

$$\det(N) = \det\left(\frac{1}{\lambda_M} M\right) = \frac{1}{\lambda_M^2} \det(M) = \frac{\det(M)}{\det(M)} = 1$$

Ainsi, l'application φ arrive bien dans $\mathrm{SL}_2(\mathbb{F}_4)$.

Soit alors $\bar{M} \in \mathrm{PGL}_2(\mathbb{F}_4)$, montrons que $\varphi(\bar{M})$ ne dépend pas du représentant $A \in \bar{M}$ choisi. Soit $k \in \mathbb{F}_4^*$, kM est un élément quelconque de la classe de M et

$$\varphi(\bar{M}) = \frac{1}{\lambda_{kM}} kM = \frac{1}{\det(kM)^2} kM = \frac{1}{k^4 \det(M)^2} kM = \frac{1}{\det(M)^2} M = \frac{1}{\lambda_M} M$$

Ainsi, $\varphi(\bar{M})$ ne dépend pas du représentant choisi et la bonne définition de l'application est assurée.

De plus, φ est un morphisme. Afin de montrer ce point, on considère $\bar{P}, \bar{Q} \in \mathrm{PGL}_2(\mathbb{F}_4)$, dont on note P et Q des représentants. Par définition du produit dans le groupe quotient, le produit des classes donne

$$\bar{P} \cdot \bar{Q} = \overline{PQ}.$$

En appliquant φ ,

$$\varphi(\bar{P} \cdot \bar{Q}) = \varphi(\overline{PQ}) = \frac{1}{\lambda_{PQ}} PQ.$$

En utilisant $\lambda_{PQ} = \det(PQ)^2$, on obtient

$$\frac{1}{\lambda_{PQ}} PQ = \frac{1}{\det(PQ)^2} PQ = \frac{1}{\det(P)^2 \det(Q)^2} PQ = \frac{1}{\lambda_P} P \frac{1}{\lambda_Q} Q = \varphi(\bar{P}) \varphi(\bar{Q})$$

Finalement, $\boxed{\varphi(\bar{P} \cdot \bar{Q}) = \varphi(\bar{P}) \varphi(\bar{Q})}$ et φ est bien un morphisme.

Montrons maintenant qu'il est injectif.

Soit $\bar{M} \in \ker \varphi$, alors $\varphi(\bar{M}) = I_2$. Par définition de φ , M est colinéaire à I_2 (via le rapport $\lambda_M \in \mathbb{F}_4^*$), et ces matrices appartiennent donc à la même classe d'équivalence dans $\mathrm{PGL}_2(\mathbb{F}_4)$. Ainsi, $\bar{M} = \bar{I}_2$ et

$$\ker \varphi = \{\bar{I}_2\}$$

Le morphisme φ est donc injectif, et ceci couplé à la propriété 2.25 (les ensembles de départ et d'arrivée ont même cardinal) montre que φ est un isomorphisme de groupes. Finalement,

$$\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{SL}_2(\mathbb{F}_4)$$

□

Forts de ce résultat, on constate que les morphismes ϕ_{SL} et ψ se comportent de la même manière, si bien que

$$\begin{aligned} \phi_{SL} : \mathrm{SL}_2(\mathbb{F}_4) &\longrightarrow \mathfrak{S}_5 \\ M &\longmapsto \psi(M) \end{aligned}$$

est lui aussi injectif.

Il s'agit maintenant d'identifier l'image du morphisme ϕ_{SL} afin de conclure à un isomorphisme de groupes. Pour cela, nous combinons plusieurs résultats antérieurs avec le théorème suivant :

Théorème 2.27 (Premier théorème d'isomorphisme).

Soient G et H deux groupes, et $f : G \rightarrow H$ un morphisme de groupes. Alors f induit un isomorphisme

$$\tilde{f} : G / \ker f \rightarrow \mathrm{Im} f$$

En conséquence, dans le cas de groupes finis, on a la relation

$$|G / \ker f| = |\mathrm{Im} f|.$$

En combinant cette conséquence avec le théorème 2.7, on obtient pour notre morphisme ϕ_{SL} que

$$|\ker \phi_{SL}| \times |\mathrm{Im} \phi_{SL}| = |\mathrm{SL}_2(\mathbb{F}_4)|.$$

Or, ϕ_{SL} est injectif, donc $\ker \phi_{SL} = \{I_2\}$ et $|\ker \phi_{SL}| = 1$. Il vient donc

$$|\mathrm{Im} \phi_{SL}| = |\mathrm{SL}_2(\mathbb{F}_4)|.$$

La propriété 2.25 donne alors $|\mathrm{Im} \phi_{SL}| = 60$, ce qui fait de $\mathrm{Im} \phi_{SL}$ un sous-groupe d'indice 2 de $\mathfrak{S}_5$ — tout comme $\mathcal{A}_5$...

Lemme 2.28.

Si H est un sous-groupe de $\mathfrak{S}_n$ d'indice 2, alors $H = \mathcal{A}_n$.

Démonstration.

Puisque H est d'indice 2,

$$|\mathfrak{S}_n/H| = 2.$$

Il existe donc deux classes possibles dans l'espace quotient, H et $T = \mathfrak{S}_n \setminus H$.

Soit $\bar{\sigma} \in \mathfrak{S}_n/H$, dont on note σ un représentant. Ainsi,

- si $\sigma \in H$,

$$\begin{cases} \sigma H = H \\ H\sigma = H \end{cases}$$

- si $\sigma \in T$,

$$\begin{cases} \sigma H = T \\ H\sigma = T \end{cases}$$

Dans tous les cas, les classes à gauche et à droite sont égales, i.e. pour tout $\sigma \in \mathfrak{S}_n$, $\sigma H = H\sigma$, et donc

$$\forall \sigma \in \mathfrak{S}_n, \sigma H \sigma^{-1} = H,$$

ce qui assure que H est distingué dans $\mathfrak{S}_n$. Par la propriété 2.21, H est donc le noyau d'un morphisme de groupes

$$\Phi : \mathfrak{S}_n \longrightarrow \text{Im } \Phi$$

surjectif par construction. En combinant à nouveau le théorème de Lagrange 2.7 et le premier théorème d'isomorphisme 2.27, on obtient la relation

$$|\text{Im } \Phi| \times |\ker \Phi| = |\mathfrak{S}_n|.$$

Or, $\ker \Phi = H$ et on peut alors réécrire la relation précédente en

$$|\text{Im } \Phi| = \frac{|\mathfrak{S}_n|}{|H|} = |\mathfrak{S}_n/H| = 2.$$

Puisque $\text{Im } \Phi$ est un groupe et qu'il est de cardinal 2, nécessairement

$$\text{Im } \Phi = \mathbb{Z}/2\mathbb{Z},$$

et Φ est alors un morphisme de groupes surjectif de $\mathfrak{S}_n$ dans $\mathbb{Z}/2\mathbb{Z}$. La propriété 1.14 nous assure finalement que $\Phi = \varepsilon$ et donc

$$\boxed{H = \ker \varepsilon = \mathcal{A}_n}.$$

□

Nous pouvons maintenant conclure quant à l'isomorphisme :

Proposition 2.29.

Les groupes $\mathrm{SL}_2(\mathbb{F}_4)$ et $\mathcal{A}_5$ sont isomorphes.

Démonstration.

Nous avons établi précédemment que le morphisme de groupes

$$\phi_{SL} : \mathrm{SL}_2(\mathbb{F}_4) \longrightarrow \mathfrak{S}_5$$

était injectif. De plus, on a montré que $|\mathrm{Im} \phi_{SL}| = 60$, ce qui en fait un sous-groupe d'indice 2 de $\mathfrak{S}_5$. Le lemme 2.28 nous assure alors que

$$\mathrm{Im} \phi_{SL} = \mathcal{A}_5,$$

et donc

$$\phi_{SL} : \mathrm{SL}_2(\mathbb{F}_4) \longrightarrow \mathcal{A}_5$$

est bijectif, ce qui conclut quant à l'isomorphisme $\boxed{\mathrm{SL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5}$. □

Il est maintenant important de faire un pas en arrière et de contempler le chemin parcouru. Initialement, nous nous étions intéressés au groupe $\mathrm{GL}_2(\mathbb{F}_4)$, car il agit sur $\mathbb{P}^1(\mathbb{F}_4) = \{\mathrm{Vect}(X) \mid X \in \mathbb{F}_4^2, X \neq 0\}$, qui correspond à l'ensemble des droites vectorielles du plan $\mathbb{F}_4^2$, au nombre de 5. L'action de ce groupe consiste à envoyer une droite vectorielle sur une autre, ce qui fait naturellement penser au groupe symétrique $\mathfrak{S}_5$, qui a pour vocation de permuter des éléments entre eux. Malheureusement, cette action n'est pas fidèle, car faire agir deux matrices distinctes, mais colinéaires, sur la même droite vectorielle d donne le même résultat.

En ce sens, on passe au quotient afin d'éliminer les redondances, regroupant par classes d'équivalence les matrices de $\mathrm{GL}_2(\mathbb{F}_4)$ qui sont identiques à homothétie près, c'est à dire colinéaires. Ceci donne naissance au groupe $\mathrm{PGL}_2(\mathbb{F}_4)$. L'action de ce groupe sur $\mathbb{P}^1(\mathbb{F}_4)$ est dorénavant fidèle, et correspond alors bien mieux au comportement du groupe symétrique $\mathfrak{S}_5$. Cependant, en tant que groupe de classes d'équivalence de matrices, $\mathrm{PGL}_2(\mathbb{F}_4)$ est peu manipulable, on cherche donc à lui trouver un groupe isomorphe plus intuitif.

En dénombrant $\mathrm{PGL}_2(\mathbb{F}_4)$, on trouve 60 classes d'équivalence distinctes. Dans le contexte ambiant de groupe symétrique, ceci fait naturellement penser au groupe alterné $\mathcal{A}_5$, lui aussi de cardinal 60. En tant que noyau du morphisme signature ε , on considère alors son pendant matriciel, le noyau du déterminant : $\mathrm{SL}_2(\mathbb{F}_4)$. Finalement, l'intuition se révèle être juste, comme en témoigne la très belle relation :

$$\boxed{\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{SL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5}$$

2.4.3 Simplicité de $\mathrm{SL}_2(\mathbb{F}_4)$

La proposition 2.29 permet d'étudier $\mathrm{SL}_2(\mathbb{F}_4)$ plutôt que $\mathcal{A}_5$ pour établir la simplicité de ce dernier. Il suffit alors de montrer que $\mathrm{SL}_2(\mathbb{F}_4)$ n'admet aucun sous-groupe distingué non trivial. Commençons par une caractérisation des sous-groupes distingués :

Propriété 2.30.

Soit G un groupe et $H < G$. Pour tout élément $x \in G$, on note $\text{Conj}(x) = \{gxg^{-1} \mid g \in G\}$ sa classe de conjugaison dans G . Soit E un système de représentants de ces classes, et l'on pose $F = E \cap H$. On a alors l'équivalence suivante :

H est distingué dans $G \iff H$ est une réunion disjointe de classes de conjugaison de G , ou plus formellement :

$$H = \bigsqcup_{x \in F} \text{Conj}(x)$$

Démonstration.

On montre le résultat par double implication.

$\Rightarrow$ Supposons d'abord que H soit distingué dans G . Ainsi,

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H.$$

En revenant à la définition d'une classe de conjugaison, on peut alors affirmer que

$$\forall x \in F \subset H, \text{Conj}(x) \subset H$$

et ainsi $\bigsqcup_{x \in F} \text{Conj}(x) \subset H$.

Pour montrer l'autre inclusion, on considère $h \in H$. Par définition du système de représentants E , il existe un unique $x \in E$ tel que $h \in \text{Conj}(x)$. Puisque H est distingué, il est stable par conjugaison, donc la classe entière de x (qui contient notamment x) est incluse dans H . Ainsi, $x \in H$. On en déduit que $x \in E \cap H = F$. Par conséquent, $h \in \bigsqcup_{x \in F} \text{Conj}(x)$, ce qui prouve l'inclusion $H \subset \bigsqcup_{x \in F} \text{Conj}(x)$. Finalement, par double inclusion

$$H = \bigsqcup_{x \in F} \text{Conj}(x).$$

$\Leftarrow$ Supposons maintenant que $H = \bigsqcup_{x \in F} \text{Conj}(x)$. De nouveau, par définition d'une classe de conjugaison,

$$\forall g \in G, \forall x \in F, g \text{Conj}(x)g^{-1} = \text{Conj}(x),$$

et donc H est stable par conjugaison, ce qui montre qu'il est distingué dans G . □

Forts de cette caractérisation, nous allons donc chercher à identifier des classes de conjugaison, et notamment leur cardinal. Le corollaire suivant s'avèrera très utile :

Corollaire 2.31.

L'on reprend les notations précédentes et on suppose dorénavant G fini. Si H est distingué dans G , alors $|H| = \sum_{x \in F} |\text{Conj}(x)|$.

Couplé au théorème 2.7, ce résultat montre qu'un sous-groupe distingué de $\mathrm{SL}_2(\mathbb{F}_4)$ ne peut exister que si une somme de cardinaux de classes de conjugaison — incluant nécessairement la classe réduite à l'identité, puisqu'on veut un sous-groupe — divise $|\mathrm{SL}_2(\mathbb{F}_4)| = 60$.

Vue comme une action de groupe de G sur H , la conjugaison a pour orbites les classes $\mathrm{Conj}(x)$ (pour $x \in F$) définies ci-dessus et pour stabilisateurs les commutants des représentants. En effet,

$$\forall x \in F, \mathrm{Stab}(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = \mathrm{Com}(x).$$

La formule des classes se reformule alors dans notre cadre :

Proposition 2.32.

Soit G un groupe. Pour tout élément $x \in G$, on note $\mathrm{Conj}(x) = \{gxg^{-1} \mid g \in G\}$ sa classe de conjugaison dans G . Soit E un système de représentants de ces classes. On a alors

$$\forall x \in E, |G| = |\mathrm{Conj}(x)| \times |\mathrm{Com}(x)|.$$

Remarque 2.33. Dans le cas de nos matrices, le commutant d'un élément $M \in \mathrm{SL}_2(\mathbb{F}_4)$ est

$$\mathrm{Com}(M) = \{N \in \mathcal{M}_2(\mathbb{F}_4) \mid MN = NM\},$$

où N n'est pas nécessairement inversible. Comme l'on conjugue M par une matrice de $\mathrm{SL}_2(\mathbb{F}_4)$, ce qui nous intéresse en réalité est

$$\mathrm{Com}(M) \cap \mathrm{SL}_2(\mathbb{F}_4),$$

noté $\mathrm{Com}^\times(M)$ et appelé commutant inversible. Pour $G = \mathrm{SL}_2(\mathbb{F}_4)$, la proposition 2.32 se réécrit alors :

$$\boxed{\forall M \in E, |\mathrm{SL}_2(\mathbb{F}_4)| = |\mathrm{Conj}(M)_{\mathrm{SL}}| \times |\mathrm{Com}^\times(M)|}$$

Ainsi, comme nous connaissons le cardinal de $\mathrm{SL}_2(\mathbb{F}_4)$ et qu'il est plus aisé de déterminer (et donc a fortiori de dénombrer) des commutants inversibles que des classes de conjugaison, nous allons judicieusement partitionner $\mathrm{SL}_2(\mathbb{F}_4)$ afin de déterminer les commutants. Nous employons pour cela la réduction de Jordan, en distinguant les formes possibles du polynôme caractéristique. Cependant, le raisonnement étant effectué sur $\mathrm{SL}_2(\mathbb{F}_4)$, nous devons préalablement montrer que la forme normale de Jordan est atteignable par conjugaison par un élément de $\mathrm{SL}_2(\mathbb{F}_4)$.

Propriété 2.34.

Soit $A \in \mathrm{SL}_2(\mathbb{F}_4)$, alors ses classes de conjugaisons dans $\mathrm{GL}_2(\mathbb{F}_4)$ et $\mathrm{SL}_2(\mathbb{F}_4)$ sont égales. Autrement dit,

$$\mathrm{Conj}(A)_{\mathrm{GL}} = \{PAP^{-1} \mid P \in \mathrm{GL}_2(\mathbb{F}_4)\} = \{QAQ^{-1} \mid Q \in \mathrm{SL}_2(\mathbb{F}_4)\} = \mathrm{Conj}(A)_{\mathrm{SL}}.$$

Démonstration.

On raisonne par double inclusion, en notant que l'inclusion réciproque est immédiate : toute matrice Q de $\mathrm{SL}_2(\mathbb{F}_4)$ étant une matrice de $\mathrm{GL}_2(\mathbb{F}_4)$, $Q A Q^{-1} \in \mathrm{Conj}(A)_{\mathrm{GL}}$. Il reste donc à montrer que $\mathrm{Conj}(A)_{\mathrm{GL}} \subset \mathrm{Conj}(A)_{\mathrm{SL}}$.

Soit $B \in \mathrm{Conj}(A)_{\mathrm{GL}}$, il existe ainsi $P \in \mathrm{GL}_2(\mathbb{F}_4)$ tel que $B = P A P^{-1}$. En réutilisant le fait que tout élément de $\mathbb{F}_4$ est un carré (montré à la propriété 2.26), il existe $\lambda \in \mathbb{F}_4^*$ tel que $\lambda^2 = \det(P)$. On pose alors $Q = \frac{1}{\lambda} P$, et un rapide calcul donne :

$$\det(Q) = \frac{1}{\lambda^2} \det(P) = \frac{\det(P)}{\det(P)} = 1,$$

ce qui assure $Q \in \mathrm{SL}_2(\mathbb{F}_4)$.

De plus, on remarque que $Q \lambda P^{-1} = \frac{1}{\lambda} P \lambda P^{-1} = I_2$, ce qui donne $Q^{-1} = \lambda P^{-1}$. Finalement,

$$Q A Q^{-1} = \frac{1}{\lambda} P A \lambda P^{-1} = P A P^{-1} = B$$

Ainsi, $B = Q A Q^{-1}$ avec $Q \in \mathrm{SL}_2(\mathbb{F}_4)$, ce qui permet d'affirmer que $B \in \mathrm{Conj}(A)_{\mathrm{SL}}$ et de conclure quant à l'égalité

$$\boxed{\mathrm{Conj}(A)_{\mathrm{GL}} = \mathrm{Conj}(A)_{\mathrm{SL}}}$$

□

Remarque 2.35. L'égalité des classes de conjugaison étant établie, on ne précisera plus le groupe par lequel on conjugue (sauf si nécessaire). On adopte alors la notation générale, pour $A \in \mathrm{SL}_2(\mathbb{F}_4)$:

$$\mathrm{Conj}(A)$$

Nous pouvons maintenant réduire sur $\mathrm{SL}_2(\mathbb{F}_4)$ sans danger. Reprenons où nous nous étions arrêté : étant de degré 2, le polynôme caractéristique d'une matrice $A \in \mathrm{SL}_2(\mathbb{F}_4)$ peut être :

- scindé à racine double
- scindé à racines simples
- irréductible sur $\mathbb{F}_4[X]$

Nous explorons donc ces trois cas pour dégager les formes normales de Jordan possibles dans $\mathrm{SL}_2(\mathbb{F}_4)$, ainsi que les commutants inversibles associés. Notons que pour χ_A irréductible, on ne peut pas utiliser la réduction de Jordan puisque celle-ci nécessite d'avoir un polynôme caractéristique scindé. Nous utiliserons alors un passage dérobé...

χ_A est scindé à racine double

Dans ce cas, il existe $\lambda \in \mathbb{F}_4$ tel que $\chi_A = (X - \lambda)^2$, d'où $\text{Sp}(A) = \{\lambda\}$ et $\det(A) = 1 = \lambda^2$. Le corps de base étant $\mathbb{Z}/2\mathbb{Z}$,

$$\begin{aligned}\lambda^2 - 1 &= 0 \\ \implies (\lambda - 1)(\lambda + 1) &= 0 \\ \implies (\lambda - 1)^2 &= 0 \\ \implies \lambda - 1 &= 0 \\ \implies \lambda &= 1\end{aligned}$$

ce qui assure que $\chi_A = (X - 1)^2$.

Si $A = I_2$, sa forme de Jordan est elle-même :

$$A_1 = A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

et son commutant inversible est $\text{Com}^\times(A_1) = \text{SL}_2(\mathbb{F}_4)$. Le cardinal de la première classe de conjugaison est donc

$$|\text{Conj}(A_1)| = \frac{|\text{SL}_2(\mathbb{F}_4)|}{|\text{SL}_2(\mathbb{F}_4)|} = 1.$$

Sinon, $A \neq I_2$ et sa forme normale de Jordan est

$$A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Identifions son commutant.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Com}(A_2)$: alors $MA_2 = A_2M$, c'est-à-dire

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},$$

ce qui nous amène au système

$$\begin{cases} a = a + c \\ a + b = b + d \\ c = c \\ d = c + d \end{cases} \iff \begin{cases} a = d \\ c = 0 \end{cases}.$$

On obtient ainsi l'inclusion $\text{Com}(A_2) \subset \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_4 \right\}$, et l'inclusion réciproque

se vérifiant par un calcul rapide, on conclut alors

$$\text{Com}(A_2) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_4 \right\}.$$

Pour obtenir le commutant inversible, il suffit d'ajouter une condition sur le déterminant :

$$\text{Com}^\times(A_2) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_4, a^2 = 1 \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_4 \right\}.$$

Il y a ainsi 4 choix pour le coefficient b , d'où

$$|\text{Com}^\times(A_2)| = 4$$

On en déduit le cardinal de la classe de conjugaison de A_2 :

$$|\text{Conj}(A_2)| = \frac{|\text{SL}_2(\mathbb{F}_4)|}{|\text{Com}^\times(A_2)|} = \frac{60}{4} = 15.$$

χ_A est scindé à racines simples

Il existe ici $\lambda, \mu \in \mathbb{F}_4$ distincts tels que $\chi_A = (X - \lambda)(X - \mu)$: la matrice A est donc diagonalisable, avec la condition $\det(A) = 1 = \lambda\mu$ sur le déterminant. La table de multiplication de $\mathbb{F}_4$ dressée plus haut (sous la définition 2.22) montre que les seules possibilités sont

$$\begin{cases} \lambda = \omega \\ \mu = \omega^2 \end{cases} \quad \text{ou} \quad \begin{cases} \lambda = \omega^2 \\ \mu = \omega \end{cases}$$

De plus, en posant $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, on a $P^{-1} = P$ et $\det(P) = -1 = 1$ (le corps de base étant toujours $\mathbb{Z}/2\mathbb{Z}$), et donc $P \in \text{SL}_2(\mathbb{F}_4)$. On remarque alors :

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = P \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} P^{-1}$$

Les deux matrices diagonales possibles ici appartiennent donc à la même classe de conjugaison. Nous conservons

$$A_3 = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$$

pour représenter cette classe. Penchons-nous maintenant sur son commutant.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Com}(A_3)$: alors $MA_3 = A_3M$, d'où

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \begin{pmatrix} a\omega & b\omega^2 \\ c\omega & d\omega^2 \end{pmatrix} = \begin{pmatrix} a\omega & b\omega \\ c\omega^2 & d\omega^2 \end{pmatrix},$$

ce qui donne

$$\begin{cases} b\omega = b \\ c = c\omega \end{cases} \iff \begin{cases} b(\omega - 1) = 0 \\ c(\omega - 1) = 0 \end{cases}$$

or, $\omega - 1 = \omega + 1 = \omega^2 \neq 0$, donc $b = c = 0$. Comme précédemment, nous avons établi une inclusion, la réciproque se vérifiant elle aussi par un rapide calcul. On a ainsi

$$\text{Com}(A_3) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_4 \right\}.$$

Le commutant inversible s'obtient en ajoutant une condition :

$$\text{Com}^\times(A_3) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_4 \text{ et } ad = 1 \right\} = \left\{ I_2, \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} \right\}$$

Le cardinal s'en déduit aisément :

$$|\text{Com}^\times(A_3)| = 3$$

et avec la formule des classes :

$$|\text{Conj}(A_3)| = \frac{|\text{SL}_2(\mathbb{F}_4)|}{|\text{Com}^\times(A_3)|} = \frac{60}{3} = 20.$$

χ_A est irréductible

Comme χ_A est unitaire et que son coefficient constant est $(-1)^2 \det(A) = \det(A) = 1$, il existe $\alpha \in \mathbb{F}_4$ tel que

$$\chi_A = X^2 + \alpha X + \det(A) = X^2 + \alpha X + 1.$$

Il reste donc à déterminer les valeurs de α pour lesquelles χ_A est irréductible.

- si $\alpha = 0$, $\chi_A = X^2 + 1 = X^2 - 1 = (X + 1)(X - 1) = (X + 1)^2$ et χ_A n'est donc pas irréductible
- si $\alpha = 1$, $\chi_A = X^2 + X + 1$. Comme vu précédemment, ω est racine de χ_A , il n'est donc pas irréductible.
- si $\alpha = \omega$ ou $\alpha = \omega^2$, on vérifie que les deux polynômes possibles sont sans racine dans $\mathbb{F}_4$. Ainsi, puisqu'ils sont de degré 2, ils sont irréductibles sur $\mathbb{F}_4[X]$.

Le cas irréductible admet donc deux polynômes caractéristiques possibles. Nous choisissons alors un représentant de leur classes de conjugaison respectives :

$$A_4 = \begin{pmatrix} \omega & 1 \\ 1 & 0 \end{pmatrix} \text{ et } A_5 = \begin{pmatrix} \omega^2 & 1 \\ 1 & 0 \end{pmatrix}.$$

Remarque 2.36. On vérifie par un rapide calcul que $\chi_{A_4} = X^2 + \omega X + 1$ et $\chi_{A_5} = X^2 + \omega^2 X + 1$.

Pour déterminer les commutants associés à A_4 et A_5 , nous utilisons un résultat d'isomorphisme.

Lemme 2.37.

Soit $A \in \text{SL}_2(\mathbb{F}_4)$. Si χ_A est irréductible, alors

$$\text{Com}(A) \simeq \mathbb{F}_4[X]/(\chi_A).$$

Démonstration.

Pour établir le résultat, raisonnons sur u , l'endomorphisme de $\mathbb{F}_4^2$ canoniquement associé à A .

Par hypothèse, χ_u est irréductible, ce qui implique que u est un endomorphisme cyclique. Ainsi, il existe $x \in \mathbb{F}_4^2 \setminus \{0\}$ tel que $(x, u(x))$ forme une base de $\mathbb{F}_4^2$. Soit alors $v \in \text{Com}(u)$. Par ce qui précède, il existe $(\alpha, \beta) \in \mathbb{F}_4^2$ tel que :

$$v(x) = \alpha x + \beta u(x)$$

et donc en posant $P_x = \alpha + \beta X$,

$$v(x) = P_x(u)(x)$$

Évaluons maintenant v en $u(x)$. Puisque u et v commutent, on obtient

$$v(u(x)) = u(v(x)) = u(P_x(u)(x)) = P_x(u)(u(x)).$$

Ainsi v et $P_x(u)$ coïncident sur la base $(x, u(x))$: ils sont donc égaux sur $\mathbb{F}_4^2$ tout entier. Nous avons ainsi montré que

$$\forall v \in \text{Com}(u), \exists P \in \mathbb{F}_4[X], v = P(u).$$

On peut alors affirmer que le morphisme d'anneaux

$$\begin{array}{ccc} \varphi : (\mathbb{F}_4[X], +, \times) & \longrightarrow & (\text{Com}(u), +, \circ) \\ P & \longmapsto & P(u) \end{array}$$

est surjectif.

Soit $P \in \ker \varphi$, alors $\varphi(P) = P(u) = 0_{\mathcal{L}(\mathbb{F}_4^2)}$. Autrement dit, $\ker \varphi$ n'est autre que l'idéal (de $\mathbb{F}_4[X]$) des polynômes annulateurs de u ; il est donc engendré par π_u , le polynôme minimal de u . De plus, par le théorème de Cayley-Hamilton, $\chi_u(u) = 0_{\mathcal{L}(\mathbb{F}_4^2)}$ et donc $\pi_u | \chi_u$. χ_u étant ici supposé irréductible, on conclut $\pi_u = \chi_u$. Finalement,

$$\ker \varphi = (\chi_u).$$

Par le premier théorème d'isomorphisme 2.27, on peut alors conclure que

$$\tilde{\varphi} : \mathbb{F}_4[X]/(\chi_u) \longrightarrow \text{Com}(u)$$

est un isomorphisme d'anneaux. En revenant aux matrices, on conclut finalement :

$$\text{Com}(A) \simeq \mathbb{F}_4[X]/(\chi_A).$$

□

Remarque 2.38. Puisque χ_A est un polynôme irréductible de $\mathbb{F}_4[X]$, $\mathbb{F}_4[X]/(\chi_A)$ est un corps, et donc $\text{Com}(A)$ aussi ! Ainsi, on a directement que toute matrice non nulle de $\text{Com}(A)$ est inversible pour $\times$.

Il ne reste plus qu'à dénombrer les éléments de $\mathbb{F}_4[X]/(\chi_A)$, puis nous concluons quant au cardinal des commutants inversibles de A_4 et A_5 . Comme on l'a déjà vu à la proposition 2.15, le quotient peut s'écrire

$$\mathbb{F}_4[X]/(\chi_{A_4}) = \mathbb{F}_4[X]/(\chi_{A_5}) = \{a + bX \mid a, b \in \mathbb{F}_4, \}.$$

Il comporte donc $4 \times 4 = 16$ éléments. En retirant 0 pour ne conserver que les inversibles, la remarque 2.38 donne alors

$$|\text{Com}(A_4) \cap \text{GL}_2(\mathbb{F}_4)| = |\text{Com}(A_5) \cap \text{GL}_2(\mathbb{F}_4)| = 16 - 1 = 15.$$

Cependant, nous avons l'habitude de chercher $\text{Com}^\times(A_4)$ et $\text{Com}^\times(A_5)$, qui sont définis comme les commutants intersectés avec $\text{SL}_2(\mathbb{F}_4)$! Contrairement à ce que l'on pourrait croire, ce n'est pas gênant ici, nous allons emprunter une voie alternative... On a vu précédemment que les classes de conjugaison d'une matrice de $\text{SL}_2(\mathbb{F}_4)$ sont égales, qu'on conjugue dans $\text{GL}_2(\mathbb{F}_4)$ ou dans $\text{SL}_2(\mathbb{F}_4)$ (à la propriété 2.34). Nous pouvons alors utiliser la formule des classes avec $\text{GL}_2(\mathbb{F}_4)$ comme groupe ambiant :

$$|\text{Conj}(A_4)_{\text{GL}}| = |\text{Conj}(A_5)_{\text{GL}}| = \frac{|\text{GL}_2(\mathbb{F}_4)|}{|\text{Com}(A_4) \cap \text{GL}_2(\mathbb{F}_4)|} = \frac{180}{15} = 12.$$

Et enfin par égalité des classes de conjugaison :

$$\boxed{|\text{Conj}(A_4)| = |\text{Conj}(A_5)| = 12}$$

Simplicité de $\text{SL}_2(\mathbb{F}_4)$

Nous avons établi que les cardinaux possibles pour la classe de conjugaison d'une matrice $A \in \text{SL}_2(\mathbb{F}_4)$ forment la famille

$$x_1 = 1, \quad x_2 = 12, \quad x_3 = 12, \quad x_4 = 15, \quad x_5 = 20,$$

et que ceux-ci vérifient bien $x_1 + x_2 + x_3 + x_4 + x_5 = 60 = |\text{SL}_2(\mathbb{F}_4)|$. Ceci nous assure que la relation de conjugaison partitionne bien l'ensemble $\text{SL}_2(\mathbb{F}_4)$.

Soit H un sous-groupe distingué de $\mathrm{SL}_2(\mathbb{F}_4)$. D'une part, H est une réunion de classes de conjugaison (voir propriété 2.30); d'autre part, en tant que sous-groupe, il contient l'identité I_2 , et donc la classe de conjugaison de I_2 tout entière. Or, cette classe est réduite à $\{I_2\}$, c'est-à-dire la classe de cardinal $x_1 = 1$. Il existe donc une partie $F \subseteq \{2, 3, 4, 5\}$ telle que

$$|H| = 1 + \sum_{i \in F} x_i.$$

Par ailleurs, le théorème de Lagrange 2.7 impose que $|H|$ divise $|\mathrm{SL}_2(\mathbb{F}_4)| = 60$.

Il suffit alors de confronter ces deux contraintes. Énumérons toutes les valeurs que peut prendre $|H|$ selon les classes ajoutées à $\{I_2\}$ (les deux classes de cardinal 12 jouant des rôles interchangeables), et vérifions à chaque fois si 60 devient divisible :

Cardinal des classes ajoutées à $\{I_2\}$	$ H $	$ H $ divise 60 ?
0	1	oui
12	13	non
15	16	non
20	21	non
12 + 12	25	non
12 + 15	28	non
12 + 20	33	non
15 + 20	36	non
12 + 12 + 15	40	non
12 + 12 + 20	45	non
12 + 15 + 20	48	non
12 + 12 + 15 + 20	60	oui

Aucun cardinal ne convient, mis à part 1 et 60, ce qui indique qu'aucun sous-groupe non trivial et distingué dans $\mathrm{SL}_2(\mathbb{F}_4)$ ne peut exister. Nous arrivons alors finalement au résultat attendu.

Théorème 2.39.

Le groupe $\mathrm{SL}_2(\mathbb{F}_4)$ est simple.

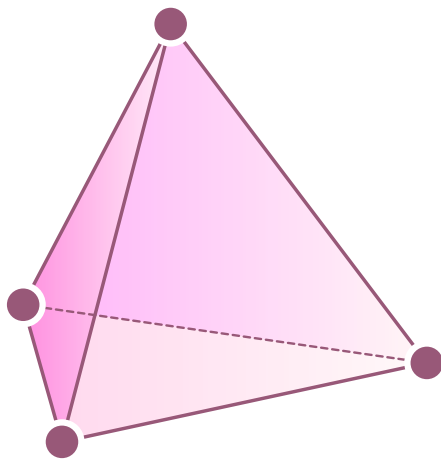
2.4.4 Conclusion

On a montré dans la partie précédente que $\mathrm{SL}_2(\mathbb{F}_4)$ est un groupe simple. L'isomorphisme exhibé à la proposition 2.29 permet alors de conclure quant à la nature de $\mathcal{A}_5$.

Théorème 2.40.

Le groupe alterné $\mathcal{A}_5$ est simple.

Cette propriété conclut l'étude de la simplicité du groupe alterné pour les cas $n \leq 5$. En plus grande dimension, on peut montrer que $\mathcal{A}_n$ est simple par récurrence sur l'entier n (voir [4]).



Bibliographie

- [1] Philippe Caldero et Jérôme Germoni, *Nouvelles histoire hédonistes de groupes et de géométries - Tome 1*, Calvage et Mounet, 2017.
- [2] Alain Debreil et Rached Mneimné, *Le groupe symétrique $\mathfrak{S}_4$ et ses métamorphoses*, Calvage et Mounet, 2026.
- [3] Philippe Caldero, *Isomorphismes exceptionnels de groupes finis*, Youtube, 2026.
- [4] Philippe Caldero, *$\mathcal{A}_n$ est simple, enfin une preuve par la réduction !*, Youtube, 2026.
- [5] *Annexe I : La géométrie élémentaire dans les mathématiques d'aujourd'hui*, du document suivant : <https://www.pedagogie.ac-aix-marseille.fr/upload/docs/application/pdf/2011-08/geometrie.pdf>