Rubik's cube et théorie des groupes

Jérôme Daquin, encadré par M^de Bhowick

Juin 2010

Table des matières

Index des notations

$\mathbf{Z}$	l' ensemble des entiers relatifs
$\mathbf{Z}_n$	l' ensemble des entiers modulo n
$\mathbf{C}$	l' ensemble des nombres complexes.
S_n	le groupe des permutations
$\varepsilon(\sigma)$	désigne la signature de la permutation σ
A_n	le groupe alterné (permutation paire de S_n)
$\|A\|$	désignera le cardinal de l' ensemble A
$\bigsqcup_{i=0}^{n} A_i$	désignera l' union disjointe des ensembles A_n
$[g,h] = ghg^{-1}h^{-1}$	dénote le commutateur
$\mathbf{Z}(G)$	le centre de G, G groupe

1 Présentation du cube de Rubik

1.1 Notation du cube

Le cube de Rubik est composé de 27 petits cubes . 26 de ces petits cubes sont visibles extérieurement. Quand on travaille avec le cube de Rubik il est utile d' avoir un moyen systématique de faire référence à un petit cube en particulier. Pour cela on donne un nom aux cubes selon leurs localisations. Les petits cubes de coins sont appelés « cubes-coins ». Chacun des 8 cubes-coins a 3 faces extérieures visibles. Les cubes avec deux faces visibles sont dits « cubes-arrêtes », ils sont au nombre de 12. Finalement les cubes n' ayant qu' une face visible sont dits « cubes-centres »,il y en a 6.

Maintenant donnons un nom à chacune des 6 faces du cube. En suivant la notation développée par David Singmaster, on les appelle right (r), left (l), up (u), down (d), back(b), front(f).

Pour nommer un cubes-coins on liste simplement les premières lettres des faces visibles ci dessus, par exemple pour faire référence au cube situé sur la face haute, à gauche dans le fond on notera ulb. Bien sur on aurait pu noter ce même cube blu ou encore lbu. On précisera la notation lors de l' introduction de l' orientation des pièces.

De façon similaire pour faire référence au cubes-centres de la face de devant on notera juste f.

Finalement on souhaite donner des noms aux mouvements du cube. Le mouvement le plus basique (mouvement élémentaire) permis par le cube de Rubik est d' effectuer une rotation d'une des 6 faces. On notera R la rotation de la face droite de 90 °dans le sens horaire (on regarde de face la face droite du cube et on la tourne de 90 °dans le sens horaire). De même on utilisera les lettres capitales L, U, D, B, F pour nommer la rotation de la face concernée. De façon générale on appellera mouvement un enchainement de ces mouvements élémentaires.

Effectuer un mouvement, c' est mélanger les couleurs du cube. Le jeu consiste à réordonner chaque cube par le biais de mouvement, de telle sorte que chaque face soit unicolore.

Un certain nombre de choses sont immédiates. On remarque qu' effectuer un mouvement élémentaire laisse invariant les cubes-centres de la face concernée. Puisque tout mouvement est un enchainement de mouvement élémentaire, chaque mouvement préserve les cubes-centres. On peut rapidement se convaincre que tout mouvement envoie un cubes-coins sur un autre cubes-coins et chaque edge cubies sur un autre edge cubies. En utilisant ces deux faits, on peut commencer à dénombrer le nombre de configurations

théoriques du cube de Rubik. Puisqu' un cube-coin s' envoie sur un cube-coin et que chaque cube-coin possède trois faces distinctes on compte $8!3^8$ possibilités de réarrangement des cubes-coins. Par le même raisonnement, on compte $12!2^{12}$ possibilités pour réarranger les edges cubies. On peut donc affirmer que le nombre de configurations du cube de Rubik est majoré par $8!3^8 12!2^{12}$ (ce nombre est de l' ordre de $5,19.10^{20}$)

Bien que ces configurations soient théoriquement possibles, cela ne veut pas dire que toutes ces configurations sont atteignables par une succession de mouvements élémentaires. Il est possible que certaines configurations théoriques ne soient pas des configurations valides, valides au sens d' atteignables par des mouvements élémentaires.

Nous avons deux buts :

1. Démontrer que certaines configurations théoriques ne sont pas valides, la modélisation mathématique du cube sera alors nécessaire.
2. Trouver un ensemble de mouvements nous permettant de résoudre le jeu.

1.2 Groupe de Rubik légal et illégal

Définition 1.1 (groupe de Rubik légal)**.** *Par groupe de Rubik, on entend le groupe engendré par les 6 mouvements élémentaires. La loi du groupe se définit ainsi : si M_1 et M_2 sont deux mouvements alors M_1M_2 sera le mouvement qui consiste à effectuer M_1 puis M_2. Dorénavant, nous noterons Rub ce groupe ; i.e $Rub = < U, D, F, B, R, L >$.*

Un mouvement licite est un mouvement s' obtenant par une suite de mouvements élémentaires. Au contraire, un mouvement illicite ou illégal est un mouvement ne s' obtenant pas par une suite de mouvements élémentaires, un mouvement illicite est obtenu par démontage du cube.

Définition 1.2 (Groupe de Rubik illégal ou élargi)**.** *Par groupe de Rubik élargi, on entend groupe de Rubik auquel on rajoute tous les mouvements illégaux possibles.On note $\overline{Rub}$ ce groupe*

Dans la suite de ce document, on va montrer entre autre que :

Proposition 1.1. *Rub est un sous groupe d' indice 12 de $\overline{Rub}$*

2 Mathématiques du cube

Le fil rouge de cette section est de caractériser exactement Rub. Pour cela on introduit suffisamment de matériaux. L' état du cube à un moment

donné dépend de :

1. La position des cubes coins
2. La position des cubes arrêtes
3. L' orientation des cubes coins
4. L' orientation des cubes arrêtes

2.1 Action des mouvements élémentaires sur les facettes du cube

On commence par assigner un numéro à chacune des facettes des cubes-coins (voir figure 1)

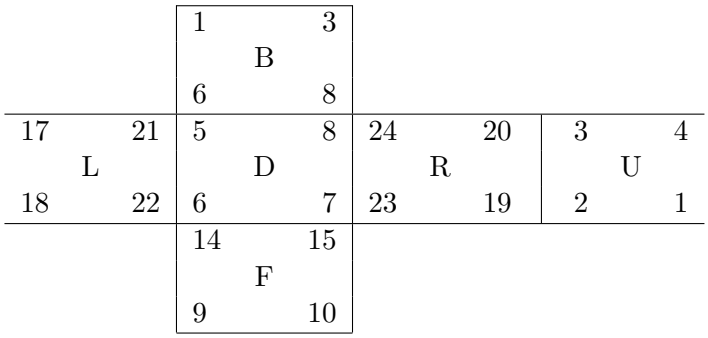

FIGURE 1 – Labelisation des cubes coins

Ecrivons la décomposition en cycle disjoint de la permutation des facettes des cubes-coins associée aux mouvements élémentaires. Nous notons σ_U la permutation associée au mouvement Up, σ_D pour la permutation associée à Down etc. Nous avons :

$$\begin{aligned}
\sigma_U &= (1,4,3,2)\quad (9,17,11,19)\quad (10,18,12,20)\\
\sigma_D &= (6,7,8,5)\quad (13,22,15,24)\quad (14,23,16,21)\\
\sigma_R &= (19,20,24,23)\quad (2,11,8,15)\quad (3,16,7,10)\\
\sigma_L &= (17,18,22,21)\quad (1,14,5,12)\quad (9,6,13,4)\\
\sigma_B &= (12,13,16,11)\quad (4,21,8,20)\quad (17,5,24,3)\\
\sigma_F &= (9,10,15,14)\quad (2,23,6,18)\quad (19,7,22,1)
\end{aligned}$$

Nous faisons la même chose pour les cubes arrêtes (voir la figure 2).

Ecrivons la décompostion en cycle disjoint de la permutation des cubes-arrêtes associée aux mouvements élémentaires. Nous avons :

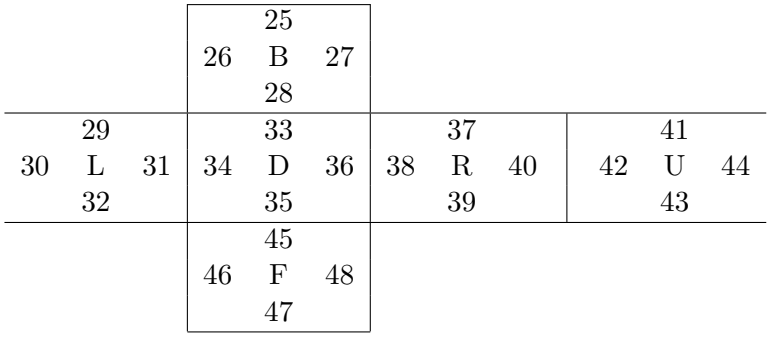

FIGURE 2 – Labelisation des cubes-arrêtes

$$\begin{aligned}
\tau_B &= (25, 26, 28, 27)\quad (41, 29, 33, 37)\\
\tau_U &= (44, 41, 42, 43)\quad (30, 25, 40, 47)\\
\tau_D &= (35, 36, 33, 34)\quad (45, 38, 28, 31)\\
\tau_R &= (37, 40, 39, 38)\quad (36, 25, 42, 47)\\
\tau_L &= (30, 32, 31, 29)\quad (44, 46, 34, 26)\\
\tau_F &= (45, 48, 47, 46)\quad (35, 39, 25, 32)
\end{aligned}$$

2.2 Action des mouvements élémentaires sur la position des cubes

Dans cette section on regarde les choses de façon moins précise : on ne distingue plus les facettes d' un même cube. On va faire le même travail que lors de la section précédente et on va introduire 3 morphismes qui vont nous permettre d' arriver à un premier résultat.

Dans la section précédente nous avions distingué les facettes d' un même cube, chose que nous ne faisons pas ici. Appuyons nous sur la section précédente pour obtenir certaines propriétés :

1. `cas des cubes-coins :` Nous avions obtenu un produit de trois 4-cycles lors de la décomposition en cycle disjoint associée aux mouvements élémentaires. En ne distinguant plus les facettes d' un même cube nous obtenons donc, en décomposant selon les mouvements élémentaires, un seul 4-cycle.
2. `cas des cubes-arrêtes :` Nous avions obtenu un produit de deux 4-cycles. En ne distinguant plus les facettes d' un même cube-arrête nous obtenons donc un seul 4-cycle.

Effectuer un mouvement g c' est permuter les pièces du cubes. Pour cela on se donne :

$$\begin{aligned} \Phi_{cube} : Rub &\to S_{20} \\ g &\mapsto \rho_g \end{aligned}$$

où ρ_g désigne la permutation des 20 cubes mobiles associée au mouvement g.

Regarder la permutation des 20 pièces mobiles, c' est regarder la permutation de 12 cubes-arrêtes disjointe de la permutation des 8 cubes-coins. Pour cela on introduit :

$$\begin{aligned} \Phi_{\text{arrête}} : Rub &\to S_{12} \\ g &\mapsto \tau_g \end{aligned}$$

et aussi

$$\begin{aligned} \Phi_{coin} : Rub &\to S_8 \\ g &\mapsto \sigma_g \end{aligned}$$

Nous arrivons à notre première proposition :

Proposition 2.1. $\Phi_{cube}(Rub) < A_{20}$

Démonstration. On commence par le vérifier pour les mouvements élémentaires. Nous avons vu que dans le cas des mouvements élémentaires la permutation σ_X était un 4-cycle et cela $\forall X \in \{U, D, R, L, B, F\}$.

$$\Rightarrow \varepsilon(\sigma_X) = -1$$

Idem concernant τ_X

$$\Rightarrow \varepsilon(\tau_X) = -1$$

Maintenant regarder la permutation ρ_X c' est regarder le produit des permutations σ_X et τ_X :

$$\rho_X = \sigma_X \, \tau_X = \tau_X \, \sigma_X \quad \forall \, X \in \{U, L, ..., B\}$$

D' où :

$$\varepsilon(\rho_X) = 1, \quad \forall \, X \in \{U, L, ..., B\}$$

La propriété est donc vraie pour les mouvements élémentaires. Maintenant on regarde le cas d' un mouvement quelconque. Un mouvement quelconque se représente comme un mot $X_1 \cdots X_k$ où les $X_i \in \{U, L, \cdots, B\}$. De plus :

$$\rho_{X_1 \ldots X_k} = \rho_{X_1} \cdots \rho_{X_k}$$

$$\Rightarrow \varepsilon(\rho_{X_1 \ldots X_k}) = \prod_{i=1}^{k} \varepsilon(\rho_{X_i}) = 1$$

et la proposition est démontrée. □

`Conséquence physique sur le cube :` la proposition 2.1 nous dit qu'il impossible de résoudre le cube sans démontage si deux et seulement deux pièces sont mal positionnées car, auquel cas, il faudrait effectuer une transposition, chose exclue par la proposition.

Corollaire 2.2. *Si un mouvement g est légal alors la permutation des coins associée à g et la permutation des cubes arrêtes associée à g ont même signature.*

Démonstration. La proposition 2.1 nous dit : $\varepsilon(\rho_g) = 1 = \varepsilon(\sigma_g)\varepsilon(\tau_g)$.

$$\Rightarrow \varepsilon(\sigma_g) = \varepsilon(\tau_g)$$

□

2.3 Orientations des cubes

2.3.1 Orientation des cubes-coins

Comme dit plus haut, un cube-coins présente trois facettes distinctes visibles extérieurement. On propose ici un moyen pour rendre compte de cette différence. Il s' agit essentiellement de fixer quelques notations. L' idée va être d' attribuer à chacune des facettes de chacun des cubes-coins un scalaire qui va être soit 0,1 ou 2. On peut penser ces scalaires comme des éléments de $\mathbf{Z}_3$

On s' imagine le cube posé sur sa face down.

On commence par attribuer une série de 0 a certaines facettes de certains cubes-coins : ces facettes sont les facettes up de la face up et les facettes down de la face down.

Ensuite on réalise le patron de la couronne up. A ce stade le patron a cette allure :

		b		
	0		0	
		U		
	0		0	
		f		

Ensuite on complète la numérotation des facettes non numérotées de chaque cubes-coins par le scalaire 1 puis 2 en partant du 0 dans le sens horaire. A ce stade le patron a exactement cette allure :

	2	**b**	1	
1	0		0	2
		U		
2	0		0	1
	1	**f**	2	

On procède de la même façon pour attribuer un numéro à chacune des facettes des cubes-coins de la face down.

Par ce procédé on vient de fixer l' orientation initiale des cubes-coins du cube. Ensuite on fixe une fois pour toute un numéro aux facettes up de la face up et aux facettes down de la face down :

- 1 pour ufl
- 2 pour ufr
- 3 pour ubr
- 4 pour ubl
- 5 pour dbl
- 6 pour dfl
- 7 pour dfr
- 8 pour dbr

Après avoir effectuer un mouvement g sur la configuration initiale, on rend compte de la nouvelle orientation ainsi : à chacune des facettes numérotées $i, i = 1 \dots 8$, on associe x_i [1] le scalaire sur la facette $i, i = 1 \dots 8$.
On définit le vecteur $f(g) = (x_1, \dots, x_8) \in \mathbf{Z}_3^8$.
$f(g)$ est donc un vecteur qui rend compte de l' orientation des cubes-coins après avoir fait subir au cube le mouvement g.

Exemple 1. *Lorsque le cube de Rubik est dans sa position initiale nous avons* $f(g) = (0, \cdots, 0)$

Exemple 2. *Calcul des vecteurs f(g) avec g un des mouvements élémentaires (voir figure 3)*

1. Il est sous entendu que chaque x_i dépend du mouvement g

$$\begin{array}{|l|}\hline \mathrm{f(R)} = (0,2,2,0,0,0,1,1) \\ \mathrm{f(L)} = (1,0,0,1,2,2,0,0) \\ \mathrm{f(U)} = (0,0,0,0,0,0,0,0) \\ \mathrm{f(D)} = (0,0,0,0,0,0,0,0) \\ \mathrm{f(B)} = (0,0,2,2,1,0,0,1) \\ \mathrm{f(F)} = (2,2,0,0,0,1,1,0) \\ \hline \end{array}$$

FIGURE 3 – Calcul des vecteurs orientations des cubes- coins

Remarque 1. *Dans l' exemple ci-dessus on peut voir que la rotation totale des vecteurs orientations est nulle :* $\sum_{i=1}^{8} x_i \equiv 0[3]$

2.3.2 Orientation des cubes-arrêtes

Cette fois-ci un cube-arrête présente deux orientations possibles. L' idée est exactement la même que dans le cas des cubes-coins. On commence par labéliser les 12 cubes-arrêtes mobiles ainsi :

- 1 pour ub de la face U
- 2 pour ur de la face U
- 3 pour uf de la face U
- 4 pour ul de la face U
- 5 pour lb de la face B
- 6 pour rb de la face B
- 7 pour rf de la face F
- 8 pour lf de la face F
- 9 pour db de la face D
- 10 pour dr de la face D
- 11 pour df de la face D
- 12 pour dl de la face D

Maintenant chacun des 12 cubes-arrêtes mobiles a une face numérotée dans chacune des 6 faces du cube. A toute ces faces on attribue 0, aux autres faces de chaque cube-arrêtes on attribue 1. Après un mouvement g on attribue a chacun des 12 cubes le chiffre $v_i = 0 \,\mathrm{ou}\, 1$ sur la face initialement numérotée i et cela pour $i = 1 \ldots 12$. On définit ainsi un vecteur $t(g) = (v_1, \ldots, v_{12})$ témoin de l' orientation des cubes-arrêtes.

`Petit récapitulatif` :

1. Se donner l' orientation des cubes coins c' est se donner un vecteur $f(g) = (x_1, \cdots, x_8) \in \mathbf{Z}_3^8$

2. Se donner l' orientation des cubes-arrêtes, c' est se donner un vecteur $t(g) = (v_1, \cdots, v_{12}) \in \mathbf{Z}_2^{12}$

2.3.3 Résultats liés à l' orientation des cubes

Nous avons deux résultats liés à l' orientation des cubes : la proposition 2.3 exprime l' orientation des vecteurs coins et arrêtes après une composition de deux mouvements, la proposition 2.4 exprime la nullité des vecteurs cubes et resp. arrêtes modulo 3 et 2 resp.

Proposition 2.3. $\forall g, h \in Rub$:

$$f(gh) = f(g) + \sigma_g.f(h)$$
$$t(gh) = t(g) + \tau_g.t(h)$$

Proposition 2.4. $\forall g \in Rub$:

$$\sum_{i=1}^{8} x_i \equiv 0[3]$$
$$\sum_{i=1}^{12} v_i \equiv 0[2]$$

On retient la proposition 2.4 en disant que les vecteurs $f(g)$ et $t(g)$ sont de rotation totale nulle.

Démonstration. De la proposition 2.3

On s' intéresse à la formule concernant les coins, la démonstration se laisse généraliser au cas des cubes-arrêtes de manière analogue.
Effectuer le mouvement gh, c' est effectuer d' abord g puis h. Le mouvement g réoriente le cube via la donnée de $f(g)$. Le mouvement h réoriente les cubes après action de σ_g sur le cube de $f(h)$. Au final on a bien : $f(gh) = f(g) + \sigma_g f(h)$ □

Démonstration. De la proposition 2.4

On ne la vérifie que dans le cas des cubes-coins. On effectue cette preuve par récurrence sur la longueur du mouvement qui, on le rappelle, peut se voir comme un mot en les lettres dans l' ensemble {U,F,...,D}.

Pour les mouvements élémentaires (mot de longueur 1) cette formule est vraie (nous avons effectué les calculs explicites voir pour cela l' exemple 3).

On suppose la propriété établie pour un mouvement de longueur k, c' est-à-dire pour un mouvement g se représentant par un mot de longueur k, $g = X_1 \cdots X_k$ où les X_i sont des éléments de l' ensemble $\{U, D, L, R, B, F\}$

Passons à un mouvement de longueur $k+1$. En utilisant la proposition 2.3, on écrit :

$$\begin{aligned} f(g) &= f(X_1 \cdots X_{k+1}) \\ &= f(X_1 \cdots X_k \, X_{k+1}) \\ &= f(X_1 \cdots X_k) + \sigma_{X_1 \cdots X_k}.f(X_{k+1}) \end{aligned}$$

Le vecteur $f(X_1 \cdots X_k)$ est un vecteur de rotation totale nulle en utilisant la formule de récurrence. $f(X_{k+1})$ est aussi un vecteur de rotation totale nulle (vecteur rotation associé à un mouvement élémentaire). Maintenant on remarque que si $f(g) = (x_1, \cdots, x_8)$ alors :

$$\sum_{i=1}^{8} x_i \equiv 0[3] \Leftrightarrow \sum_{i=1}^{8} x_{\sigma(i)} \equiv 0[3], \quad \forall \sigma \in S_8$$

D' où :

$$f(g) = \underbrace{f(X_1 \cdots X_k)}_{\text{rot. nulle}} + \underbrace{\sigma_{X_1 \cdots X_k}.f(X_{k+1})}_{\text{rot.nulle}}$$

est un vecteur de rotation totale nulle comme somme de deux vecteurs de rotation totale nulle. Cela achève la preuve. □

Nous allons modéliser *Rub* comme un produit direct de produit semi-directs. Pour cela nous effectuons un aparté sur les produits semi-directs.

2.4 Produit semi-direct

Définition 2.1 (Action de groupe sur un ensemble)**.** *Une action d' un groupe G sur un ensemble X est la donnée d' une application :*

$$\begin{aligned} f : G \times X &\to X \\ (g, x) &\mapsto g * x \end{aligned}$$

satisfaisant à :

1. $e_g.x = x \quad \forall\, x \in X$
2. $g_1.(g_2.x) = g_1 g_2.x$

Se donner une action est équivalent à se donner un morphisme de groupe $\phi : G \to S_X$. S' il en est ainsi on dira que G agit sur X ou que X est muni d' une action de G.

Définition 2.2. *Soit H et K deux groupes. On suppose H muni d' une action de K. On définit sur $H \times K$ une loi interne notée * :*

$$(h,k) * (h',k') = (h\ k.h', kk')$$

*Cette loi * confère à $(H \times K, *)$ une loi de groupe et $(H \times K, *)$ est dit produit semi-direct de H par K pour cette action et est noté $H \ltimes K$.*

`anticipation : application au cube de Rubik`
S_8 agit sur $\mathbf{Z}_3^8$ de la façon suivante :

$$\mathbf{Z}_3^8 \times S_8 \to \mathbf{Z}_3^8$$
$$(x = (x_1, \cdots, x_8), \sigma) \mapsto \sigma.x \overset{not}{=} \sigma x = (x_{\sigma(1)}, \cdots, x_{\sigma(8)})$$

et de la même façon : S_{12} agit sur $\mathbf{Z}_2^{12}$

$$\mathbf{Z}_2^{12} \times S_{12} \to \mathbf{Z}_2^{12}$$
$$(t = (v_1, \cdots, v_{12}), \sigma) \mapsto \sigma.t \overset{not}{=} \sigma t = (v_{\sigma(1)}, \cdots, v_{\sigma(12)})$$

On munit donc le produit $S_n \times \mathbf{Z}_k^n$ d' une loi de groupe * ainsi :

$$(S_n \times \mathbf{Z}_k^n) \times (S_n \times \mathbf{Z}_k^n) \to S_n \times \mathbf{Z}_k^n$$
$$(\sigma_1, f_1) * (\sigma_2, f_2) \mapsto (\sigma_1\sigma_2, f_1 + \sigma_1 f_2)$$

On peut donc définir deux nouveaux morphismes :

$$\Gamma_{coin} : Rub \to S_8 \ltimes \mathbf{Z}_3^8$$
$$g \mapsto (\sigma, f)$$

et

$$\Gamma_{\text{arrête}} : Rub \to S_{12} \ltimes \mathbf{Z}_2^{12}$$
$$g \mapsto (\tau, t)$$

qui permettent de rendre compte de l' évolution de la position et de l' orientation des cubes-coins et arrêtes où :

- σ désigne la permutation des coins associée à g
- f l' orientation des cubes-coins
- τ la permutation des coins-arrêtes associée à g
- t l' orientation des cubes-arrêtes

En recollant les morceaux on obtient :

$$\begin{aligned}\Psi : Rub \to &(\mathbf{Z}_3^8 \ltimes S_8) \times (\mathbf{Z}_2^{12} \ltimes S_{12}) \\ g \mapsto &(\sigma, f, \tau, t)\end{aligned}$$

Exemple 3. *En adoptant les notations ci-dessus, la position initiale du cube de Rubik s' écrit* $(1, 0, 1, 0)$ *où il faut lire :*

- *Le premier* 1 *du 4-uplet comme* 1_{S_8} *: tout les cubes-coins sont à la bonne position.*
- *Le premier* 0 *du 4-uplet comme* 0 *de* $\mathbf{Z}_3^8$ *: tout les cubes-coins sont correctement orientés.*
- *Le second* 1 *du 4-uplet comme* $1_{S_{12}}$ *: tout les cubes-arrêtes sont à la bonne position.*
- *Le second* 0 *du 4-uplet comme* 0 *de* $\mathbf{Z}_2^{12}$ *: tout les cubes-arrêtes sont correctement orientés.*

La section suivante à pour idée de caractériser *Rub* en fonction de ce 4-uplets.

2.5 Structure du cube

L' état du cube à un moment donné dépend de :

1. la position et l' orientation des cubes-coins
2. la position et l' orientation des cubes-arrêtes

Donnons nous donc un 4-uplets (σ, f, τ, t) avec $\sigma \in S_8, \tau \in S_{12}$, $f \in \mathbf{Z}_3^8$ et t $\in \mathbf{Z}_2^{12}$. La question est la suivante : à quelles conditions ce 4-uplets est-il représentatif d' un mouvement licite ? Nous allons répondre à cette question en affirmant qu' un tel 4-uplets est représentatif d' un mouvement licite, si et seulement si

a) $\varepsilon(\sigma) = \varepsilon(\tau)$

b) $\sum_{i=1}^{8} x_i \equiv 0[3]$

c) $\sum_{i=1}^{12} v_i \equiv 0[2]$

2.5.1 Théorème fondamental du cube

Théorème 2.1 (théorème fondamental du cube)**.** *Un mouvement g de* $\overline{Rub}$ *est licite si et seulement si le 4-uplets associé à g vérifie les contraintes a) , b) et c) mentionnées ci-dessus.*

Démonstration. Donnons nous un mouvement g licite auquel on fait correspondre le 4-uplets (σ, f, τ, t) . Concernant l' égalité de la signature c' est le corollaire 2.2. Concernant la nullité des vecteurs orientations c' est la proposition 2.4

Réciproquement on se donne un 4-uplets (σ, f, τ, t) satisfaisant les contraintes ci-dessus. On veut voir que ce 4-uplets est représentatif d' un mouvement g légal (g élément de Rub), c 'est à dire que notre 4-uplets est dans l' orbite légale de la position initiale $(1, 0, 1, 0)$. Notre problème est donc de passer de (σ, f, τ, t) à $(1, 0, 1, 0)$ de façon légale. La preuve est assez constructive et repose sur ces 4 propositions.

Proposition 2.5 (Positionnement des cubes-coins)**.** *Si (σ, f, τ, t) est une configuration satisfaisant les contraintes a), b) et c) alors il existe un mouvement légal M tel que l' action de M sur l' état du cube à pour conséquence de mener le cube dans une configuration du type $(1, f', \tau', t')$.*

Proposition 2.6 (Orientation des cubes-coins)**.** *Si $(1, f, \tau, t)$ est une configuration satisfaisant les contraintes alors il existe un mouvement légal M tel que l' action de M sur l' état du cube à pour conséquence de mener le cube dans une configuration du type $(1, 0, \tau', t')$.*

Proposition 2.7 (Positionnement des cubes-arrêtes)**.** *Si $(1, 0, \tau, t)$ est une configuration satisfaisant les contraintes alors il existe un mouvement légal M tel que l' action de M sur l' état du cube à pour conséquence de mener le cube dans une configuration du type $(1, 0, 1, t')$.*

Proposition 2.8 (Orientation des cubes-arrêtes)**.** *Si $(1, 0, 1, t)$ est une configuration satisfaisant les contraintes alors il existe un mouvement légal M tel que l' action de M sur l' état du cube à pour conséquence de mener le cube dans une configuration du type $(1, 0, 1, 0)$.*

Si on accepte l' ensemble de ces propositions alors la preuve est achevée. □

Le problème est de prouver les propositions de 2.5 à 2.8. C' est ce que nous faisons donc maintenant.

Lemme 2.1 (Pour la proposition 2.5)**.** *L' application $\Phi_{coin} : Rub \to S_8$ est surjective.*

Démonstration. On rappelle que S_n est engendré par les transpositions de S_n. S_8 est donc engendré par les transpositions de S_8. Il suffit donc de voir que $Im\Phi_{coin}$ contient toutes les transpositions.

$Im\Phi_{coin}$ en contient déjà une car le mouvement $M_0 = ([D, R]F)^3$ échange 2 coins (dbr urb) et fixe tous les autres.

Par conjugaisons $Im\Phi_{coin}$ les contient toutes, explicitons. En effet soit C_1 et C_2 deux cubes coins quelconques. Il existe un mouvement légal qui envoie dbr sur C_1 et urb sur C_2. On a alors :

$$\begin{aligned}\Phi_{coin}(M^{-1} \quad M_0 \quad M) &= \Phi_{coin}(M)^{-1} \quad \Phi_{coin}(M_0) \quad \Phi_{coin}(M) \\ &= \sigma^{-1}(\text{dbr urb})\sigma \\ &= (\sigma(dbr) \quad \sigma(urb)) \\ &= (C_1 \quad C_2)\end{aligned}$$

□

Démonstration. (de la proposition 2.5) Par le lemme, il existe un mouvement M tel que $\Phi_{coin}(M) = \sigma^{-1}$. Il suffit alors d' appliquer le mouvement M à notre cube pour que l' ensemble de nos cubes-coins soient correctement positionné. □

Lemme 2.2. *(pour la proposition 2.6) Si C_1 et C_2 sont deux cubes coins, il existe un mouvement M légal qui change l' orientation de C_1 et de C_2 et qui n' affecte aucun autre cube-coins.*

Démonstration. L' idée est d' abord de trouver un mouvement M satisfaisant le lemme puis de conjuguer ce mouvement pour agir sur n' importe quel autre cubes-coins. Le mouvement

$$M_0 = (DR^{-1})^3(D^{-1}R)^3$$

admet la décomposition en cycle disjoint suivante :

$$(dfr, rdf, frd)(drb, rbd, bdr)(df, dr, fr, ur, br, db, dl).$$

Ainsi $\Phi_{coin}(M_0) = 1$ et tous les autres cubes coins bien sont non-affectés. Donc si $C_1 = dbr$ et $C_2 = drf$ alors le lemme est vrai. Quitte à conjuguer ce mouvement M_0 comme tout à l' heure par un mouvement M envoyant dbr sur C_1 et drf sur C_2 on a le résultat. De plus $M' = M^{-1}M_0M$ fait subir une rotation horaire à C_1, anti-horaire à C_2 □

Démonstration. (de la proposition 2.6) On suppose notre cube de Rubik avec au moins deux cubes-coins C_1 et C_2 ayant une orientation mauvaise. Grâce au lemme précédent, il existe un mouvement M licite qui fait tourner

C_1 de façon horaire, C_2 de façon anti-horaire et n' affectant aucun autre cube-coins. En appliquant ce mouvement encore une fois (si nécessaire), on peut assurer que C_1 est correctement orienté. Puisque le mouvement n' affecte aucun autre cube, tous nos cubes sauf peut-être un (C_2) est mal-orienté. Deux cas :

1. C_2 est correctement orienté et dans ce cas la preuve est terminée
2. C_2 est mal orienté. En réalité ce cas ne peut envisagé car il contredirait la formule 2.4

Au final tous nos cubes-coins sont correctement orientés. □

A ce stade tous nos cubes-coins sont correctement orientés et positionnés. Maintenant on traite le cas des cubes-arrêts de façon très similaire. Pour prouver la formule 2.7 nous allons utiliser des mouvements n' affectant ni l' orientation ni la position des cubes-coins (i.e des éléments de $Ker\,\Gamma_{coin}$).

Lemme 2.3. *(pour la proposition 2.7) L' image de* $\Phi_{arrête}|Ker\,\Gamma_{coin}$: $Ker\,\Gamma_{coin} \to S_{12}$ *contient* A_{12}

Démonstration. On sait que A_{12} est engendré par les 3-cycles de A_{12}. Le mouvement :

$$M_0 = LR^{-1}U^2L^{-1}RB^2$$

admet pour décomposition (ub, uf, db). Donc M_0 appartient bien à $Ker\,\Gamma_{coin}$ et $\Phi_{\text{arrête}}(M_0) = (ub, uf, db)$. Quitte à conjuguer comme précédemment on a le résultat. □

Démonstration. (de la proposition 2.7) immédiat grâce au lemme (cf proposition 2.5) □

Il ne nous reste plus qu' à orienter de façon correcte tous les cubes-arrêtes sans affecter les autres-cubes. On a besoin d' un analogue du lemme nous ayant servit pour la proposition 2.6.

Lemme 2.4. *(pour la proposition 2.8) Si* C_1 *et* C_2 *sont deux cubes-arrêtes, il existe un mouvement qui change l' orientation de* C_1 *et de* C_2 *sans affecter les autres cubes. Le mouvement* M_0 *suivant satisfait aux conditions recherchées :*

$$M_0 = LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$$

La décomposition de ce mouvement en cycle est : $(fu, uf)(bu, ub)$. *De plus nous savons que l' action de Rub sur les triplets* (C_1, C_2, C_3) *est transitive.*

En particulier si C_1 et C_2 sont deux cubes-arrêtes, il existe un mouvement M envoyant uf sur C_1 et ub sur C_2. Le mouvement $M^{-1}M_0M$ change l' orientation de C_1 et de C_2 et n' affecte aucun autre cube.

Démonstration. (de la proposition 2.8) similaire à la preuve de 2.6 □

On a donc démontré le théorème fondamental du cube et cette preuve contient un algorithme de résolution du cube.

Corollaire 2.9. *Le groupe de Rubik Rub est donné par :*

$$Rub \simeq \{(\sigma, f, \tau, t) \in (\mathbf{Z}_3^8 \ltimes S_8) \times (\mathbf{Z}_2^{12} \ltimes S_{12}) |\ a)\ ,\ b)\ et\ c)\ sont\ vraies\ \} = \mathcal{A}$$

Démonstration. C' est une re-traduction du théorème fondamental du cube. □

La multiplication d' un élément de $\mathcal{A}$ est contenue dans la section concernant les produits semi-directs. Quand on parle d' un élément g de *Rub* on ne voit pas g comme un mot en les lettres U,F,...,D mais plutôt comme son 4-uplets représentatif.

Corollaire 2.10. *Le centre de Rub comprend 2 éléments : l' identité et l' élément*[2] $z = (\sigma, f, \tau, t)$ *avec* $t = (1, \ldots, 1) \in \mathbf{Z}_2^{12}$, $f = (0, \ldots, 0) \in \mathbf{Z}_3^8$ $\sigma = id_{S_8}$ *et* $\tau = id_{S_{12}}$.

Démonstration. Soit g et g' deux éléments de Rub que l' on identifie au produit direct de nos deux produits semi-directs. Ecrivons $g = (\sigma, f, \tau, t)$ et $g' = (\sigma', f', \tau', t')$. Nous cherchons donc les éléments g satisfaisant à $gg' = g'g \quad \forall\ g' \in Rub$. Nous avons :

$$gg' = (\sigma\sigma', f + \sigma.f', \tau\tau', t + \tau.t') \tag{1}$$
$$g'g = (\sigma'\sigma, f' + \sigma'.f, \tau'\tau, t' + \tau'.t) \tag{2}$$

De plus, de la simplicité du groupe $A_n, n > 4$ nous tirons que les seuls sous-groupes distingués de $S_n, n > 4$ sont A_n, S_n lui même et le groupe trivial $\{e\}$. Le centre d' un groupe est bien sur distingué dans ce même groupe. C' est pourquoi de l' égalité (1) et de l' égalité (2) nous tirons que :

$$\sigma \in \mathbf{Z}(S_8) = \{e\}$$

et de la même facon que :

$$\tau \in \mathbf{Z}(S_{12}) = \{e\}$$

2. L' élément z est dit le superflip

ensuite nous devons satisfaire :

$$f + f' = f' + \sigma' f \tag{3}$$
$$t + t' = t' + \tau' f' \tag{4}$$

L' équation (3) force à ce que $f = (0, \ldots, 0)$, $f = (1, \ldots, 1)$ ou $f = (2, \ldots, 2)$. Puisque la rotation de f doit être nulle, automatiquement $f = (0, \ldots, 0)$. De la même façon, l' équation (4) force à ce que $t = (0, \ldots, 0)$ ou $t = (1, \ldots, 1)$. Nous avons bien démontré le résultat annoncé. □

2.5.2 Conséquences

Nous allons nous appuyer sur le travail préliminaire pour déterminer le cardinal de *Rub*. Pour cela on introduit : $\mathcal{C} = \{(\sigma, f, \tau, t) \quad |\text{a') et b') sont vraies}\}$ où :

a') $\sum_{i=1}^{8} x_i \equiv 0[3]$

b') $\sum_{i=1}^{12} v_i \equiv 0[2]$

Nous définissons l' opération suivante sur $\mathcal{C}$:

$$\mathcal{C} \times \mathcal{C} \to \mathcal{C}$$
$$(\sigma, f, \tau, t).(\sigma', f', \tau', t') \mapsto (\sigma\sigma', f + \sigma.f', \tau\tau', t + \tau.t')$$

Cette opération fait de $\mathcal{C}$ un groupe. C' est un sous-groupe de $\overline{Rub}$ d' indice 6 comme le dit le théorème suivant.

Théorème 2.2. *Nous avons l' isomorphisme suivant :*

$$\mathcal{C} \simeq (\mathbf{Z}_3^7 \ltimes S_8) \times (\mathbf{Z}_2^{11} \ltimes S_{12})$$

Nous avons besoin d' un lemme pour faire cette preuve.

Lemme 2.5. *Soit* $E_0 = \{(x_1, \ldots, x_n) \in (\mathbf{Z}_k)^n \quad | \sum_{i=1}^{n} \equiv 0[k])$. *Nous avons* $|E_0| = k^{n-1}$

Démonstration. On introduit : $E_p = \{(x_1, \ldots, x_n) \in (\mathbf{Z}_k)^n \quad | \sum_{i=1}^{n} \equiv p[k])$ et on considère :

$$f_p : E_0 \to E_p$$
$$(x_1, \ldots, x_n) \mapsto (x_1 + p, \ldots, x_n)$$

f_p est correctement définie et est bijective. Cela implique que $|E_0| = |E_p|$. De plus :

$$(\mathbf{Z}_k)^n = \bigsqcup_{p=0}^{k-1} E_p$$

D' où : $k^n = k.|E_0| \Rightarrow |E_0| = k^{n-1}$ □

Démonstration. (du théorème) Grâce au lemme on identifie les éléments satisfaisant a') à $\mathbf{Z}_3^7$ et les éléments satisfaisant b') à $\mathbf{Z}_2^{11}$. □

Corollaire 2.11. *Le cube de Rubik Rub est le noyau du morphisme suivant :*

$$\Phi : \mathcal{C} \to \{-1, 1\}$$
$$(\sigma, f, \tau, t) \mapsto \varepsilon(\sigma)\varepsilon(\tau)$$

En particulier , $Rub \lhd \mathcal{C}$ d' ordre 2 et

$$|Rub| = 8!.3^7.12!.2^{10}$$

ce qui fait de Rub un sous-groupe d' indice 12 *de* $\overline{Rub}$

Démonstration. C' est clair. □

2.5.3 Mouvements d' ordre 2

On se propose dans cette section de déterminer le cardinal de l' ensemble des mouvements d' ordre 2 de *Rub*.

Plaçons nous dans S_n. Le nombre de cycles de longueur k distincts vaut $\frac{n(n-1)...(n-k+1)}{k}$. Le coefficient $\frac{1}{k}$ sert à ne pas compter plusieurs fois un même k-cycle : $(i_1, i_2, i_3, \dots) = (\dots, i_1, i_2, i_3, \dots)$. En particulier le nombre de 2-cycle (transposition) dans S_n vaut $\frac{n(n-1)}{2}$. Supposons n > 4, le nombre d' élément dans S_n du type (ab)(cd) (produit de deux transpositions) vaut :

$$\frac{\frac{n(n-1)(n-2)(n-3)}{2\times 2}}{2!}$$

Le coefficient $\frac{1}{2!}$ sert à ne pas compter deux fois les mêmes produits : $(i_1 i_2)(i_3 i_4) = (i_3 i_4)(i_1 i_2)$.

Plaçons maintenant dans $\mathbf{Z}_3^7 \ltimes S_8$. Un élément (x, σ) y est d' ordre deux si et seulement si nous avons $(x, \sigma)(x, \sigma) = (x + \sigma x, \sigma^2) = (1, 1)$. Ainsi σ est un produit de transpositions et nous devons satisfaire :

$$x_i + x_{\sigma(i)} \ = 0[3], \forall i \in \ \{1, \dots, 8\}$$

nature	cardinal
transpositions	$\frac{8\times 7}{2}$
produit de deux transpositions	$\frac{1}{2!}\frac{8\times 7}{2}\frac{6\times 5}{2}$
produit de trois transpositions	$\frac{1}{3!}\frac{8\times 7}{2}\frac{6\times 5}{2}\frac{4\times 3}{2}$
produit de quatre transpositions	$\frac{1}{4!}\frac{8\times 7}{2}\frac{6\times 5}{2}\frac{4\times 3}{2}\frac{2\times 1}{2}$

FIGURE 4 – éléments d' ordre 2 dans S_8

$x_i + x\sigma(i) = 0$ lié à une ...	choix possible
...transposition	3
...produit de deux transpositions	3^2
...produit de trois transpositions	3^3
...produit de quatre transpositions	3^4

FIGURE 5 – élément d' ordre 2 dans $\mathbf{Z}_3^7$

Nous avons calculer le nombre d' éléments d' ordre 2 dans S_8 (voir figure 4) . Que vaut le nombre d' éléments d' ordre 2 dans $\mathbf{Z}_3^7$? Nous devons satisfaire $x_i + x_{\sigma(i)}$ nul modulo trois. Par exemple si σ est une transposition, on peut supposer que son support est $\{1, 2\}$ et dans ce cas nous avons trois choix pour f. En effet $f = (0, \ldots, 0)$ convient, ou $f = (1, 2, 0, \ldots, 0)$ et enfin $f = (2, 1, 0, \ldots, 0)$. Nous obtenons le tableau 5. Résumons :

Le nombre d' éléments $(x, \sigma) \in \mathbf{Z}_3^7 \ltimes S_8$ d' ordre 2 avec σ paire vaut :

$$\frac{1}{4!}C_2^8 C_2^6 C_2^4 C_2^2 3^4 + \frac{1}{2!}C_2^8 C_2^6 3^2 = 10395 \tag{5}$$

Le nombre d' éléments $(x, \sigma) \in \mathbf{Z}_3^7 \ltimes S_8$ d' ordre 2 avec σ impaire vaut :

$$\frac{1}{3!}C_2^8 C_2^6 C_2^4 3^3 + C_2^8 3 = 11424 \tag{6}$$

Si on se place maintenant dans $\mathbf{Z}_2^{11} \ltimes S_{12}$ par le même raisonnement nous obtenons :

Le nombre d' éléments $(t, \tau) \in \mathbf{Z}_2^{11} \ltimes S_{12}$ d' ordre 2 avec τ paire vaut :

$$\frac{1}{6!}C_2^{12} C_2^{10} \ldots C_2^2 2^6 + \frac{1}{4!}C_2^{12} C_2^{10} \ldots C_2^6 2^8 + \frac{1}{2!}C_2^{12} C_2^{10} 2^{10} = 15491520 \tag{7}$$

Le nombre d' éléments $(t, \tau) \in \mathbf{Z}_2^{11} \ltimes S_{12}$ d' ordre 2 avec τ paire vaut :

$$\frac{1}{5!}C_2^{12} C_2^{10} \ldots C_2^4 2^7 + \frac{1}{3!}C_2^{12} C_2^{10} \ldots C_2^8 2^9 + C_2^{12} 2^{11} = 15214848 \tag{8}$$

Par le théorème fondamental du cube, nous obtenons qu' un élément (f, σ, t, τ) est d' ordre deux si et seulement c' est un élément d' ordre 2 dans le groupe $\mathcal{C} = (\mathbf{Z}_3^7 \ltimes S_8) \times (\mathbf{Z}_2^{11} \ltimes S_{12})$ et si de plus $\varepsilon(\sigma) = \varepsilon(\tau)$. Un élément non trivial $(c_1, c_2) \in \mathcal{C}$ avec $c_1 = (f, \sigma)$ et $c_2 = (t, \tau)$ est d' ordre deux si et seulement si nous sommes dans l' un des cas exclusifs suivant :

1. $c_1 \neq 1, c_2 = 1, c_1^2 = 1, \varepsilon(\sigma) = 1$
2. $c_1 = 1, c_2 \neq 1, c_2^2 = 1, \varepsilon(\tau) = 1$
3. $c_1 \neq 1, c_2 \neq 1, c_1^2 = c_2^2 = 1, \varepsilon(\sigma) = 1 = \varepsilon(\tau)$
4. $c_1 \neq 1, c_2 \neq 1, c_1^2 = c_2^2 = 1, \varepsilon(\sigma) = -1 = \varepsilon(\tau)$

On compte chaque cas. Le cas 1. est compté via (5). Le cas 2. est compté via (7). Le cas 3. est compté via (7) et (5). Le cas 4. est compté via (8) et (6)

En sommant tout cela, nous trouvons que le nombre d' éléments d' ordre 2 dans *Rub* vaut $334864275867 = (3.3\dots) \times 10^{11}$.

3 Quelques sous-groupe du groupe de Rubik

Concernant le cube de Rubik il est connu que :

1. Tout groupe non abélien de cardinal inférieur à 26 est isomorphe à un sous-groupe de Rub.
2. Tout groupe de cardinal inférieur à 13 est isomorphe à un sous-groupe de Rub.

C' est donc vrai pour le groupe $\mathcal{Q}$ des quaternions, où nous explicitons à titre d' exemple l' isomorphisme.

3.1 Sous-groupe des quaternions

Nous effectuons quelques rappels sur $\mathcal{Q}$ puis montrons la présence de ce dernier au sein de *Rub*.

Définition 3.1. $\mathcal{Q} :=< a, b >$ *où* $a^4 = 1$, $b^2 = a^2$, *et* $aba = b$

Proposition 3.1. $\mathcal{Q}$ *est d' ordre 8, non commutatif.*

Démonstration. On peut écrire la table du groupe en utilisant les relations rappelées dans la définition de $\mathcal{Q}$.

□

Proposition 3.2. *On a l' isomorphisme suivant :*

$$\mathcal{Q} \simeq \mathcal{Q}^* \ = < a_0, b_0 >$$

où :

$$a_0 = F^2 M_R U^{-1} M_R^{-1} U^{-1} M_R U M_R^{-1} U F^2$$
$$b_0 = F U^2 F^{-1} U^{-1} L^{-1} B^{-1} U^2 B U L$$

Démonstration. On définit :

$$\begin{aligned} q : \mathcal{Q}^* &\to \mathcal{Q} \\ a_0 &\mapsto q(a_0) = a \\ b_0 &\mapsto q(b_0) = b \end{aligned}$$

On vérifie informatiquent que a_0 et b_0 satisfont les contraintes définissant $\mathcal{Q}$. □

3.2 Two-faces group

On va s' intéresser dans cette section à un sous groupe de *Rub* engendré par deux mouvements élémentaires à savoir U et F. Nous allons introduire le plan projectif $\mathbf{P}(\mathbf{F}_5)$ dans le but de montrer qu' il existe un moyen de labéliser les sommets des faces U et F comme des éléments de $\mathbf{P}(\mathbf{F}_5)$ afin d' interpréter l' action des mouvements élémentaires sur les sommets des faces U et F comme une transformation homographique à coefficient dans $\mathbf{F}_5$.

Définition 3.2. *Soit $p \in \mathcal{P}$ l' ensemble des nombres premiers. On définit le plan projectif $\mathbf{P}(\mathbf{F}_p)$ comme :*

$$\mathbf{P}(\mathbf{F}_p) = \{0, 1, \cdots, p-1, \infty\}$$

Définition 3.3 (transformation de Möbius / Homographie)**.** *Si $a, b, c, d \in \mathbf{F}_p$ non tous nuls, on définit la transformation de Möbius ou encore dite transformation homographique par :*

$$\begin{aligned} f : \mathbf{P}(\mathbf{F}_p) &\to \mathbf{P}(\mathbf{F}_p) \\ x &\mapsto \frac{ax+b}{cx+d} \end{aligned}$$

Définition 3.4. *On note* $\mathbf{GL}(2,\mathbf{F}_5)$ *l' ensemble des matrices* 2×2 *à coefficient dans* $\mathbf{F}_5$ *inversibles. Ce groupe agit naturellement sur* $\mathbf{P}(\mathbf{F}_5)$ *comme suit :*

$$\begin{aligned}\mathbf{GL}(2,\mathbf{F}_5)\times\mathbf{P}(\mathbf{F}_5)&\to\mathbf{P}(\mathbf{F}_5)\\ (\begin{pmatrix} a & b\\ c & d\end{pmatrix},x)&\mapsto\frac{ax+b}{cx+d}\end{aligned}$$

Définition 3.5. *Le sous-groupe de* $\mathbf{GL}(2,\mathbf{F}_p)$ *constitué des matrices ayant pour déterminant 1 est dit sous-groupe spécial linéaire. On note* $\mathbf{SL}(2,\mathbf{F}_p)$ *ce groupe.*

Proposition 3.3. *Le centre de* $\mathbf{GL}(2,\mathbf{F}_p)$ *est donné par :*

$$Z(\mathbf{GL}(2,\mathbf{F}_p))=\{\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}|a\in\mathbf{F}_p,\,a\ non\ nul\}:=\mathcal{A}$$

Démonstration. L' inclusion de l' ensemble $\mathcal{A}$ dans le centre est évidente. Montrons l' autre inclusion. Supposons donc que :

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} r & s\\ u & v\end{pmatrix}=\begin{pmatrix} r & s\\ u & v\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

pour tout a,b,c,d. Cela implique $bu=cs\quad\forall b,c$. Cela est impossible sauf si $u=s=0$. Cela force $cr=cv\quad\forall\, c$. Cela implique $r=v$. Cela prouve l' inclusion recherchée. □

Définition 3.6. *Le groupe quotient* $\mathbf{PGL}(2,\mathbf{F}_p)=\mathbf{GL}(2,\mathbf{F}_p)/Z(\mathbf{GL}(2,\mathbf{F}_p))$ *est dit groupe projectif linéaire.*
Le groupe quotient $\mathbf{PSL}(2,\mathbf{F}_p)=\mathbf{SL}(2,\mathbf{F}_p)/Z(\mathbf{SL}(2,\mathbf{F}_p))$ *est dit groupe projectif spécial linéaire.*

Théorème 3.1 (interprétation homographique de U et F)**.** *Il existe des scalaires appartenant à* $\mathbf{F}_5$ *et une façon de labéliser les sommets des faces U et F par des éléments de* $\mathbf{P}(\mathbf{F}_5)$ *de telle sorte que :*

1. *L' action du mouvement élémentaire F sur les sommets des faces U et F soit la même que l' action de la transformation homographique* f_F *définie ci-dessous sur les éléments de* $\mathbf{P}(\mathbf{F}_5)$ *:*

$$f_F(x)=\frac{x-1}{x+1}$$

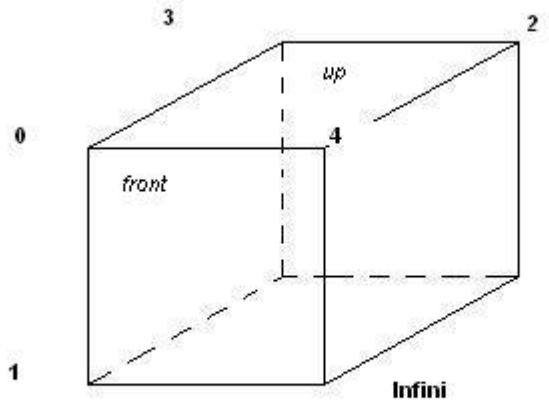

FIGURE 6 – Labelisation des sommets avec les éléments du plan projectif

2. *L' action du mouvement élémentaire U sur les sommets des faces U et F soit la même que l' action de la transformation homographique f_U définie ci-dessous sur les éléments de* $\mathbf{P}(\mathbf{F}_5)$ *:*

$$f_U(x) = 3x + 3$$

Démonstration. On labélise les sommets comme dans la figure 6. Avec cette labélisation nous avons $\sigma_F = (0, 4, \infty, 1)$ et $\sigma_U = (0, 3, 2, 4)$ et cela est en accord avec la définition donnée à f_U et f_F. □

Soit :

$$\begin{aligned} \Phi :< F, U > \to &< f_F, f_U > \quad < \quad \mathbf{PGL}(2, \mathbf{F}_5) \\ F &\mapsto f_F \\ U &\mapsto f_U \end{aligned}$$

Φ est surjective et nous avons :

Théorème 3.2. $\mathbf{PGL}(2, \mathbf{F}_5) \simeq < f_F, f_U >$

Démonstration. Notons

$$\begin{pmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{pmatrix}_{\bullet} \in \mathbf{PGL}(2, \mathbf{F}_5)$$

l' image de

$$\begin{pmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{pmatrix}$$

sous le morphisme

$$\begin{aligned} \mathbf{GL}(2, \mathbf{F}_5) &\to \mathbf{PGL}(2, \mathbf{F}_5) \\ g &\mapsto \mathbf{F}_5^{\times}.g \end{aligned}$$

Puique $f_U^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_{\bullet}$ nous avons $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_{\bullet} \in < f_U, f_F >$.

Puisque $f_F.f_U^5 = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}_{\bullet}$ nous avons que $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}_{\bullet} \in < f_U, f_F >$.

En conjuguant cette matrice par f_U^2, nous trouvons que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_{\bullet} \in < f_U,\ f_F >$.

Nous savons que $\mathbf{SL}(2, \mathbf{F_5})$ est engendré par les transvections élémentaires, d' où :

$$\mathbf{PSL}(2, \mathbf{F_5}) \quad < \quad < f_U, f_F > \quad < \quad \mathbf{PGL}(2, \mathbf{F_5})$$

Nous avons :

$$|\mathbf{PSL}(2, \mathbf{F_5})| = 60 \,\text{et que}\, |\mathbf{PGL}(2, \mathbf{F_5})| = 120$$

Pour conclure, il suffit d' exhiber un élément de $< \ f_U,\ f_F \ >$ qui n' est pas élément de $\mathbf{PSL}(2, \mathbf{F_5})$. Un tel élément est f_U. En effet, le déterminant de f_U appartient à l' ensemble $3.(\mathbf{F}_5^{\times})^2 = \{3x^2 \,|\, x \in \mathbf{F}_5\}$. Mais un élément de $\mathbf{PSL}(2, \mathbf{F}_5)$ doit avoir un déterminant valant 1. Puisque aucun élément de $\mathbf{F}_5$ satisfait à $3x^2 = 1$ nous sommes en mesure de conclure que f_U n' appartient pas à $\mathbf{PSL}(2, \mathbf{F}_5)$ et cela achève la preuve. □