Le groupe du Rubik's Cube
(Tome I)

La connaissance est le patrimoine de l'humanité, donc chaque être humain peut l'utiliser librement mais il a aussi le devoir de le protéger, partager, améliorer.

Morphocode CODE

Titre: Le groupe du Rubik's Cube (Tome I)

Auteur: Morphocode CODE

Site web: https://fan2cube.fr

Version: 17.3-24.8.29

ISBN : 979-8-4484-5266-6

Préface

J'ai découvert le Rubik's Cube dans une boutique à jouer, pendant les grandes vacances d'été 2007...

Le Rubik's Cube dans la main ... par curiosité, pour voir comment ça marche, j'ai donc fait quelques rotations ... et puis j'ai essayé de le remettre en ordre, mais plus j'essayais plus je mélangeais le Cube ! plus j'éloignais de mon but !! et finalement il m'était impossible de le remettre à l'état origine, mon Cube était complètement mélangé !

C'est extraordinaire, impressionnant quelques rotations seulement et il est impossible de le restaurer !! J'ai donc dû acheter des livres de résolutions, un tas de livres .... et finalement j'ai réussi à remonter le Cube, tout ça grâce aux livres.

Et je m'entraînais à résoudre le Cube sans les notes sous les yeux, sans les livres, j'apprenais les formules par cœur ...

Et puis un jour j'ai remarqué quelque chose d'étrange et intrigante .

Au dernier étage de la résolution, l'algorithme fonctionne comme suite:

1. On place les 4 arêtes Haut.

2. On pivote ces arêtes pour les bien orientées.

3. On place les sommets

4. On pivote les sommets pour bien orientés.

Ce que j'ai remarqué est la chose suivante:

I. Dans l'étape (2): On pivote toujours deux arêtes, jamais une !! pourquoi ?

II. A l'étape (3) , il y a 4 sommets déjà bien placés ou 3 sommets à placer , pourquoi jamais deux sommets à échanger comme dans l'étape (1) ? . Pourquoi on tombe jamais sur deux sommets à échanger ??

III. A l'étape (4) on pivote toujours :

- soit deux sommets dans le sens contraire

- soit trois sommets dans le même sens ?

Pourquoi on ne pivote jamais un sommet ?

Ca m'a vraiment intrigué, j'ai cherché des explications partout, ... peu de livres en parlent.

Et beaucoup plus tard j'ai appris que ça provient des propriétés mathématiques du Cube, ce qui m'a beaucoup intéressé car j'aime beaucoup les maths. A partir de là j'ai beaucoup lu, un tas de livres, un tas d' articles traitant sur le côté mathématique du Cube ...

Le Rubik's Cube est célèbre non seulement c'est un casse-tête redoutable mais aussi parce qu'il concrétise physiquement une théorie mathématique abstrait: Les Groupes.

Ce livre explique tout ce qui se passe de la face cachée du Cube ...

Il vous explique pourquoi:

1. On ne peut pas pivoter une arête sans rien toucher les autres arêtes.
2. On ne peut pas pivoter un sommet sans rien toucher les autres sommets.
3. On ne peut pas permuter deux arêtes sans rien toucher les sommets.
4. On ne peut pas pivoter un centre à ±90° sans rien toucher les autres pièces.
5. ...

1 LES GROUPES

L'étude mathématique du Rubik's Cube s'appuie énormément sur la notion de groupe, donc il faut bien connaître cette notion, mais il n'est pas question de refaire la théorie des groupes ici ! car il existe des livres pour ça. On va donc donner un résumé : les définitions, les théorèmes, les propriétés ... dont on a besoin. Mais je vous conseille vivement de faire un tour sur la théorie des groupes car c'est le bon moment, un bon prétexte pour connaître cette théorie.

Soit G un ensemble, muni une loi notée '.' on dit que (G,.) est un groupe si la loi '.' vérifie 4 propriétés suivantes :

1. a,b dans G $\Rightarrow$ a.b $\in$G (loi interne)
2. il existe un élément e tel que a.e = e.a = a (e = élément neutre)
3. pour chaque a, il existe a^{-1} tel que $a.a^{-1} = a^{-1}.a = e$ (a^{-1} = symétrique de a, ou inverse de a)
4. (a.b).c = a.(b.c) (associative)

De plus si on a : a.b = b.a (commutative) On dit que G est un groupe commutatif ou abélien.
Remarque : parfois on écrit: ab = a.b et et 1 = e

Attention !! '1' , 'a^{-1}' ce sont des simples notations, des symboles, des caractères, rien à voir avec le nombre entier 1 , et les inverses: $3^{-1} = \frac{1}{3}$ par ex.

Sous-groupe

Soit H un sous ensemble d'un groupe G, $H \subset G$ on dit que H est un sous groupe si:

1. $e \in H$

2. $x \in H \Rightarrow x^{-1} \in H$

3. $x,y \in H \Rightarrow xy \in H$

ou bien

1. $H \neq \emptyset$

2. $\forall x,y \in H \Rightarrow xy^{-1} \in H$

Un sous groupe est dit normal (ou distingué) si

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

Les sous groupes normaux sont très recherchés car ils permettent de 'diviser' G c'est-à-dire K = G/H , K est un groupe. Lorsque H n'est pas normal on ne peut pas diviser G par H par contre on peut former ce qu'on appelle les classes de H.

Les classes de H

Définition : Soit H un sous groupe (pas forcement normal) de G, on appelle la classe Hg gauche (H est à gauche) de G, l'ensemble :

$Hg = \{x \in G \mid x = hg \text{ , où } h \in H\}$; $g \in G$ donné, fixé

C'est donc les éléments $x \in G$ de la forme $x = hg$ où $h \in H$, et $g \in G$ donné, fixé. L'ensemble des classes gauches est noté:

$H\backslash G = \{Ha, Hb, Hc, ... \}$; $a,b,c, ... \in G$ donnés, fixés

Les classes à droite (H à droite):

$gH = \{x \in G \mid x = gh \text{ , où } h \in H\}$; $g \in G$ donné, fixé

$G\backslash H = \{aH, bH, cH, ... \}$; $a,b,c, ... \in G$ donnés, fixés

* H est normal $\Leftrightarrow$ $H\backslash G = G\backslash H$ classes à gauche = classes à droite .

Trois propriétés importantes :

1. $|H| = |Hg|$, une classe a le même nombre d'éléments que H.

2. $|H\backslash G| = |G|/|H|$;

3. Les classes forment une partition de G.

Même chose pour les classes à droite

Homomorphisme ou morphisme

Soient (E, .) et (F, .) deux groupes, on dit que f est un homomorphisme si f respecte les lois.

$f: E \to F$

$f(xy) = f(x)f(y)$

Propriétés :

* $f(e) = e$

en effet

$f(x) = f(ex) = f(e)f(x)$ et

$f(x) = f(xe) = f(x)f(e)$

ce qui montre que $f(e) = e$

* $f(x^{-1}) = (f(x))^{-1}$

en effet

$f(xx^{-1}) = f(x)f(x^{-1})$

$f(e) = f(x)f(x^{-1})$

$e = f(x)f(x^{-1})$

et

$f(x^{-1} x) = f(x^{-1})f(x)$

$f(e) = f(x^{-1})f(x)$

$e = f(x^{-1})f(x)$

d'où $f(x-1) = (f(x))^{-1}$

Attention !! soyez très prudent , il faut savoir qui est qui, où on met les pieds, on est dans où ? dans E où dans F ?? ...

dans l'écriture $f(e) = e$, le 'e' à gauche c'est l'élément neutre de G et celui de droite c'est l'élément neutre de F, de même

$f(xy) = f(x)f(y)$

$f(x.y) = f(x).f(y)$ le '.' à gauche c'est la loi dans G et celui '.' de droite c'est la loi dans F.

Dans l'écriture mathématique, parfois on écrit des abréviations, mais si on simplifie trop on ne comprend rien ! si on écrit tout c'est trop lourd impossible à décoder ... Bref il faut savoir mesurer pas tout écrit, pas trop simplifier non plus .....

Si f est bijective on dit que f est un isomorphisme.

Un isomorphisme de E dans E est un automorphisme, bref ce sont des vocabulaires à connaître c'est tout.

Noyau , Image de f

$Ker(f) = \{ x \in G \mid f(x) = e \}$

* Ker(f) est normal.

* Si H est normal, alors H est le noyau de quelqu'un,
H = Ker(f)

* Ker(f) = {e} ⇒ f = injectif

* Im(f) = f(G) = {y∈F |∃x∈G , f(x) = y} est un sous groupe de F

* G/Ker(f) = Im(f) ; un théorème bien connu

* Si f est injective ⇔ Ker(f) = {e} ⇒ E/{e} = Im(f) ⇒ E= Im(f) ça signifie que E ⊂ F

<u>Sous groupe engendré</u>

X sous ensemble de G.

Le sous groupe engendré par X: < X > par définition:

* Le plus petit sous groupe contenant X

ou

* L'intersection de tous les sous groupes contenant X

* Les produits du type $X \cup X^{-1}$

ex:
$(\mathbb{Z},+)$ est un groupe (abélien)
$(\mathbb{Q}^*,x)$ est un groupe, lui aussi abélien
$(\mathbb{Z}_7,+)$ est un groupe abélien
(S_n,o) est un groupe
etc .... il y a beaucoup de groupes en mathématique.

Exemple important

On pose :

$K = S_n \times \mathbb{Z}_k^n$

un élément μ de K est donc $\mu = (u,x)$, $u \in S_n$, $x \in \mathbb{Z}_k^n$

Les éléments de K se nomment les configurations

$uu' = u' \circ u$

$x = (x_1 , x_2, ..., x_n)$; $x_i \in \mathbb{Z}_k$

$u(x) = (x_{u(1)}, x_{u(2)} , ... , x_{u(n)})$

Propriété:

$u(x+y) = u(x) + u(y)$.

En effet

$u(x) + u(y) = (..., x_{u(i)} , ...) + (..., y_{u(i)} , ...)$

$= (..., x_{u(i)} + y_{u(i)} , ...) = (..., (x + y)_{u(i)} , ...) = u(x+y)$

On définit sur K une loi '.' suivante:

$\mu = (u,x)$, $\mu' = (u',x')$

$\mu\mu' = (u,x)(u',x') = (uu', x+u(x'))$

Voyons si (K, .) forme un groupe.

1) C'est visiblement une loi interne.

2) e = (id,0)

(u,x)(id,0) = (u.id, x+u(0)) = (u, x+0) = (u,x)

(id,0)(u,x) = (id.u, 0+id(x)) = (u, 0+x) = (u,x)

(id,0) est l'élément neutre.

3) Soit (u,x) , et on prend $(u^{-1}, u^{-1}(-x))$

$(u,x)(u^{-1}, u^{-1}(-x)) = (uu^{-1}, x + u\,u^{-1}(-x)) = (id, x + id(-x)) =$

$= (id, x -x) = (id,0) = e$

$(u^{-1}, u^{-1}(-x))\ (u,x) = (u^{-1}\,u,\ u^{-1}(-x) + u^{-1}(x)) = (id, u^{-1}(x-x)) =$

$= (id, u^{-1}(0)) = (id,0) = e$

Chaque élément (u,x) a une symétrique $(u^{-1}, u^{-1}(-x))$,

4) a: (u,x)(u',x') = (uu', x+u(x'))

(uu', x+u(x')) (u'',x'') = (uu'u'', x+u(x') + uu'(x''))

b: (u',x')(u'',x'') = (u'u'',x'+u'(x''))

(u,x)(u'u'',x'+u'(x'')) = (uu'u'', x+ u(x'+u'(x''))

= (uu'u'', x+ u(x')+uu'(x''))

on a bien (μμ')μ'' = μ(μ'μ'')

(K, .) est bien un groupe.

Exo:
1. $(\mathbb{N}, .)$ où la loi ' . ' est définie par: a.b = ppcm(a,b)
questions:
a. la loi '.' est-elle interne ?
b. la loi '.' est-elle associative ?
c. y a t-il un élément neutre ?

2. $(\mathbb{N}, .)$ où la loi ' . ' est définie par: a.b = pgcd(a,b)
questions:
a. la loi '.' est-elle interne ?
b. la loi '.' est-elle associative ?
c. y a t-il un élément neutre ?

3. $(\mathbb{R}-\{1\}, .)$ où la loi ' . ' est définie par: a.b = a+b-ab
a. la loi '.' est-elle interne ?
b. $(\mathbb{R}-\{1\}, .)$ est-il un groupe ?

4. $(\mathbb{R}, .)$ où la loi ' . ' est définie par: $a.b = \ln(e^a+e^b)$
questions:
a. la loi '.' est-elle interne ?
b. la loi '.' est-elle associative ?
c. y a t-il un élément neutre ?

5. $( ]-1,1[, .)$ où la loi ' . ' est définie par: $a.b = (a+b)/(1+ab)$
questions:
a. est-il un groupe ?

6. (G, .) un groupe, montrer que si on a : $a^2 = e$ pour tout a, alors (G, .) est abélien

2 ACTION D'UN GROUPE SUR UN ENSEMBLE

Soient G un groupe et X un ensemble, une action '•' (à droite) de G sur X est une loi externe de X x G -→ X vérifiant 2 propriétés:

X x G -→ X
(x,g) -→ x•g = x'∈X

1. ∀x ; x•e = x (e = élément neutre de G)
2. ∀x, g, h ; (x•g)•h = x•(gh)

Attention aux notations , car parfois cela peut troubler l'esprit !!! par exemple certains auteurs notent :

$A+\vec{u} = B$

additionner un point à un vecteur pour donner un point c'est assez troublant ! car on sait seulement additionner deux vecteurs ...

$\vec{u} + \vec{v} = \vec{w}$

il fallait noter

$A \bullet \vec{u} = B$

ce serait plus clair, le vecteur $\vec{u}$ agit sur le point A pour donner le point B car les vecteurs E=espace vectoriel , agissent sur les points, le groupe (E,+) agit sur le plan $\mathcal{P}$.

¤ compatible (Rubik's Cube, X un groupe)

$\forall x, g, h$; $x\bullet(gh) = (x\bullet g)(x\bullet h)$

¤ libre (Rubik's Cube)

$a \in X$, donné, fixé

$\forall g$, $a\bullet g = a \Rightarrow g = e$

libre : e est le seul à posséder des points fixes .

¤ fidèle

$u \in G$ donné

$(\forall x$; $x\bullet u = x) \Rightarrow u = e$

fidèle : e est le seul à fixer tout le monde.

$u \in G$; $(\forall x$; $x\bullet u = x)$: signifie que u fixe tout le monde.

libre $\Rightarrow$ fidèle.

¤ transitive

$\forall x,x'$ $\exists g$ tel que $x\bullet g = x'$

On peut toujours passer de x à x'.

¤ simplement transitive (espace affine)

∀x,x' ∃!g tel que x•g = x'

Il y a une seule façon de passer de x à x'

on a: simplement transitive = transitif + libre

Exemple : La définition d'un espace affine n'est pas très claire dans la plus part des livres, voici un rappel :

Soient X un ensemble et E un esv, On dit que X est un espace affine sur E si le groupe (E,+) agit simplement transitive sur X, autrement dit s'il existe une action '•' vérifiant:

X x E -→ X
$(A,\vec{u})$ -→ $A\bullet\vec{u} = B$
1. $A\bullet\vec{0} = A$
2. $(A\bullet\vec{u})\bullet\vec{v} = A\bullet(\vec{u}+\vec{v})$
3. ∀ A,B ∃!$\vec{u}$ tels que $A\bullet\vec{u} = B$

Se donner une action '•' de G sur X, revient à se donner un morphisme ζ de (G, .) dans (S_x, .) , '.' : uu' = u' o u

ζ: G -→ S_x ; S_x = l'ensemble des permutations de X (des bijections de X)

g -→ ζ_g (une permutation de X)[1]

---

[1] $\zeta_g : X \to X$
$x \to \zeta_g(x) = x\bullet g$

qui vérifie :

1) $\zeta_e = id$

2) $\zeta_{gh} = \zeta_g \zeta_h$

Trois définitions importantes

1. Orbite : soit $a \in X$ un élément de X
$X_a = \{x \in X \mid \exists g \in G , a \bullet g = x\}$ les x qu'on peut atteindre (à partir de a) par les éléments de G, $X_a \subset X$

La relation d'équivalence $\sim$ défini par
$x \sim y \Leftrightarrow \exists g \mid x \bullet g = y$
Les classes de $\sim$ sont des orbites donc les orbites forment une partition de X.

2. Points fixes de g : soit $g \in G$ un élément de G
$F_g = \{x \in X \mid x \bullet g = x\}$ les points fixes de g , $F_g \subset X$

Orbites, points fixes $\subset X$, ils sont dans X.

3. Stabilisateur : soit $a \in X$ un élément de X
$G_a = \{g \in G \mid a \bullet g = a\}$ les g qui ne bougent pas a, les g trop "faible" pour a ; G_a = les faibles de a , $G_a \subset G$; G_a est un sous-groupe mais pas forcement normal.

Stabilisateurs $\subset G$

Deux formules :
1. $|X_a| = |G_a \backslash G| = |G|/|G_a|$

2. $\mathcal{N} = \frac{1}{|G|} \sum_{g \in G} |F_g|$

$\mathcal{N}$ = nombre d'orbites = nombre de choix = nombre de contraintes .

3 OPÉRATION MODULO

On se donne un nombre premier p , pour fixer les idées on va prendre p = 7. Dans $\mathbb{Z}$ les nombres entiers on va définir une opération suivante nommée "modulo 7" et notée %7, 10%7 c'est le reste de la division 10 par 7 donc:

10%7 = 3
14%7 = 0
5%7 = 5
2%7 = 2
8%7 = 1
-1%7 = 6
-5%7 = 2
etc....

Note: au lieu de noter 10%7 = 3 on préfère noter
10 = 3 (mod 7) donc
14%7 = 0 ⇒ 14 = 0 (mod 7)
etc ...

Exo
Calculer
21 = ? (mod 7)
15 = ? (mod 7)
7 = ? (mod 3)
6 = ? (mod 3)
-1 = ? (mod 7)
-5 = ? (mod 3)

3.1 CALCULE DANS ($\mathbb{Z}_P$,+)

On note $\mathbb{Z}_p$ l'ensemble des restes de la division d'un entier n par p, pour nous c'est $\mathbb{Z}_7$ = {0,1,2,3,4,5,6}. Sur $\mathbb{Z}_7$ on va définir une opération (l'addition) notée '+' de façon suivante:
a + b = c
où c vaut:
a + b = c (mod 7)

on note aussi

a + b = c (dans $\mathbb{Z}_7$)
ex:

3 + 5 = 1 (dans $\mathbb{Z}_7$)

car
3 + 5 = 1 (mod 7)

4 + 6 = 3 (dans $\mathbb{Z}_7$)
2 + 3 = 5 (dans $\mathbb{Z}_7$)
1 + 6 = 0 (dans $\mathbb{Z}_7$) ⇒ donc 6 est l'opposé de 1 (6 = -1)
etc .....

La table addition '+' de $\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

De même on définit $\mathbb{Z}_5 = \{0,1,2,3,4\}$. Sur $\mathbb{Z}_5$ on définit une addition notée '+' de façon suivante:
a + b = c
où c vaut:
a + b = c (mod 5)

on note aussi

a + b = c (dans $\mathbb{Z}_5$)
ex:

3 + 3 = 1 (dans $\mathbb{Z}_5$)

car
3 + 3 = 1 (mod 5)

2 + 6 = 3 (dans $\mathbb{Z}_5$)
2 + 1 = 3 (dans $\mathbb{Z}_5$)
1 + 4 = 0 (dans $\mathbb{Z}_5$) ⇒ donc 4 est l'opposé de 1 (4 = -1)
etc .....

La table addition '+' dans $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Exo

1. Dans $\mathbb{Z}_7$, quel est l'opposé de 4 ? càd -4 = ??
et -5 = ??

2. Calculer dans $\mathbb{Z}_5$

4+8 = ? , 3+1 = ? , -7+2 = ? , 4+2 = ? , -7-4 = ?

3. Donner le tableau d'addition de $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\mathbb{Z}_{11}$

3.2 CALCULE DANS ($\mathbb{Z}_P$,X)

Dans le même ordre idée on va définir une autre opération (la multiplication) notée 'x' dans $\mathbb{Z}_7$ de façon suivante:
a x b = c
où c vaut:
a x b = c (mod 7)

ex
2 x 5 = 3 (dans $\mathbb{Z}_7$)
car
2 x 5 = 3 (mod 7)

3 x 6 = 4 (dans $\mathbb{Z}_7$)
3 x 4 = 5 (dans $\mathbb{Z}_7$)
2 x 4 = 1 (dans $\mathbb{Z}_7$) ⇒ donc 4 est l'inverse de 2 ($4 = \frac{1}{2}$)

etc. .....

La table de multiplication 'x' dans $\mathbb{Z}_7$

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

De même on définit la multiplication notée 'x' dans $\mathbb{Z}_5$ de façon suivante:
a x b = c
où c vaut:
a x b = c (mod 5)

ex
2 x 7 = 4 (dans $\mathbb{Z}_5$)
car
2 x 7 = 4 (mod 5)

3 x 6 = 3 (dans $\mathbb{Z}_5$)
3 x 4 = 2 (dans $\mathbb{Z}_5$)
2 x 3 = 1 (dans $\mathbb{Z}_5$) ⇒ donc 3 est l'inverse de 2 ($3 = \frac{1}{2}$)

La table de la multiplication 'x' dans $\mathbb{Z}_5$

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exo
1. Dans $\mathbb{Z}_7$, quel est l'inverse de 3 ? càd 1/3 = ??
et 1/6 = ??

2. Dans $\mathbb{Z}_5$, quel est l'inverse de 3 ? càd 1/3 = ??
et 1/2 = ??

3. Donner le tableau de la multiplication de $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\mathbb{Z}_{11}$

4 PERMUTATIONS

On se donne n objets X = {a,b,c,d, ...} et n trous, les objets sont dans les trous. Une permutation c'est un déplacement de ces objets (dans ces trous, on ne déplace pas les objets à extérieur des trous !) et elle sera notée

p = [p(a),p(b),p(c),p(d), ...] ex:

X = {1,2,3,4,5,6,7,8}

p = [1,5,8,6,3,7,2,4]
ça signifie: p(1) = 1, p(2) = 5, p(3) = 8, p(4) = 6, p(5) = 3, p(6) = 7, p(7) = 2, p(8) = 4

q = [2,5,7,4,1,8,6,3]
ça signifie: q(1) = 2, q(2) = 5, q(3) = 7, q(4) = 4, q(5) = 1, q(6) = 8, q(7) = 6, q(8) = 3

r = [3,4,5,1,2,6,7,8]
ça signifie: r(1) = 3, r(2) = 4, r(3) = 5, r(4) = 1, r(5) = 2, r(6) = 6, r(7) = 7, r(8) = 8

r = (1,3,5,2,4) ; notation cycle

r(1)=3, r(3)=5, r(5)=2, r(2)=4, r(4)=1 ; les autres ne bougent pas

Note: lorsqu'il n'y a pas d'ambigu on peut supprimer les virgules et même les '[' , ']'

[1,5,8,6,3,7,2,4] = [15863724] = 15863724

On note S_n, ou S_x l'ensemble des permutations à n objets. Une permutation n'est rien d'autre qu'une bijection de X (donc rien de compliqué). Sur S_n on définit une loi '.'
p.q = q o p (o = rond = composition des fonctions)
on dit que '.' est le "produit" , (S_n, .) forme un groupe.

Propriétés de la loi '.'

1. p, q permutations ⇒ p.q permutation

2. permutation identique: id = (a) = (b) = ...

3. pour toute permutation p , il existe une permutation inverse p^{-1} : $p.p^{-1} = p^{-1}.p = id$

4. (p.q).r = p.(q.r) associatif

NOTE : parfois on écrit p.q = pq (on supprime le '.' on est paresseux !!) ,
soit p une permutation , on note p(x) = x.p lire "p appliquer à x" , on fait de gauche à droite, ex
pq(4) = 4.pq = (4.p)q = 6.q = q(6) = 8
pq(2) = 2.pq = (2.p)q = 5.q = q(5) = 1

on fait p puis q, on applique x à gauche

Les k-cycles

k objets se déplacent en cycle se nomme un k-cycle et on le

Note:
p = (a,b,c) ou encore a→b→c ça signifie: a va en b, b va en c, et c va en a, autrement dit: p(a) = b, p(b) = c, p(c) = a . C'est un 3-cycle, sa longueur = 3
p = (a,b) = a→b = a↔b un 2-cycle (permuter a,b ; échanger a,b ; transposer a,b ....) longueur = 2 (nombre de lettres) . On dit aussi une transposition (a,b)
p = (a) = a→a = id = identité , un 1-cycle , longueur = 1

Attention !! (1,2,3) est différent de [1,2,3]

p = (1,2,3) $\Longrightarrow$ p(1)=2, p(2)=3, p(3)=1

p = [1,2,3] = id $\Longrightarrow$ p(1)=1, p(2)=2, p(3)=3

par ex

p = (4,2,1,3,5) ⇒ p(4) = 2

q = [4,2,1,3,5] ⇒ q(4) = 3

p ≠ q

et l'écriture [a,b,c] impose d'écrire tous les éléments de X, alors que (a,b,c) non.

p = (7,2,4,1,3) = [3,4,7,1,5,6,2,8]

Cycles disjoints

Définition : On dit que deux cycles sont disjoints s' ils n'ont pas d'éléments en commun. Ex
(a,b,c)(d,e)(f,g) disjoint
(a,b,c)(c,a,d) non-disjoint , 'c', 'a' en commun

Propriété :
si p et q , deux cycles disjoints alors: pq = qp ils se commutent

Théorème 1:
Toute permutation p est décomposable en produits de cycles disjoints et la décomposition est unique.

Démonstration :
$p = (a,p(a),p^2(a), ...) (b,p(b),p^2(b), ...) (....)$

ex
X={1,2,3,4,5,6,7,8}
p = [3,2,4,1,8,5,6,7] est décomposé en produit des cycles

$p(1)=3, p(3)=4, p(4)=1 \rightarrow (1,3,4)$

$p(2)=2$

$p(5)=8, p(8)=7, p(7)=6, p(6)=5 \rightarrow (5,8,7,6)$

p = [3,2,4,1,8,5,6,7] = (1,3,4)(5,8,7,6) ; les cycles se notent entre les parenthèses.

p = [3,4,5,1,2,6,8,7] et q = (3,4,5,1,2,6,8,7)

[3,4,5,1,2,6,8,7] ≠ (3,4,5,1,2,6,8,7)

car p(2) = 4 et q(2) = 6

Note: lorsqu'il n'y a pas d'ambigu on peut supprimer les parenthèses et les virgules.

(3,4,5,1,2) = 34512

[3,4,5,1,2] = [34512]

Théorème 2 :
Toute permutation est décomposable en produits de transpositions (2-cycle) et la décomposition n'est pas unique, mais la parité du nombre de transpositions est la même.

Démonstration : il suffit de remarquer qu'on a:

(a,b,c,d) = (a,b)(a,c)(a,d) ; distributivité

(a,b,c,d) = (d,c)(c,b)(b,a) ; relation de Charles

un cycle s' exprime en transpositions.

Les 2-cycles engendrent donc S_n

Propriété :

Les transpositions de type (1,k) se nomment les transpositions unitaires.

La famille des transpositions unitaires (1,2), (1,3), ..., (1,n) engendre S_n

$S_n = < (1,2), (1,3), ... , (1,n) >$

Démonstration :

Il suffit de remarquer que :

(a,b) = (1,a)(1,b)(1,a)

ex :

$S_6 = < (1,2),(1,3),(1,4),(1,5),(1,6) >$

Propriété :

Les transpositions du type (k,k+1) se nomment les transpositions propres . La famille des transpositions propres : (1,2), (2,3), ... , (n-1,n) engendre S_n

$S_n = < (1,2), (2,3), ... , (n-1,n) >$

Démonstration :

Il suffit d'exprimer les transpositions unitaires (1,k) en fonction des transpositions propres .

on a:

(1,k) = (k-1,k)(1,k-1)(k-1,k)

on recommence avec le cycle milieu (1,k-1) ,

(1,k-1) = (k-2,k-1)(1,k-2)(k-2,k-1)

on recommence avec le cycle milieu (1,k-2) ,

(1,k-2) = (k-3,k-2)(1,k-3)(k-3,k-2)

....

(1,2)

ex:

(1,5) = (4,5)(1,4)(4,5)

(1,4) = (3,4)(1,3)(3,4)

(1,3) = (2,3)(1,2)(2,3)

finalement

(1,5) = (4,5)(3,4)(2,3)(1,2)(2,3)(3,4)(4,5)

ex :

S_6 = < (1,2),(2,3),(3,4),(4,5),(5,6) >

Propriété :

S_n engendré par deux générateurs :

S_n = < (1,2), (1,2,3, ... , n) >

Démonstration :

il suffit d'exprimer les transpositions propres en fonctions des générateurs (1,2), (1,2,3, ..., n) .

On a:

$(k,k+1) = (1,2,3, ...,n)^{(k-1)} (1,2) ((1,2,3, ...,n)^{(k-1)})^{-1}$

ex :

S_6 = < (1,2),(1,2,3,4,5,6) >

Exo
1. Montrer que :

(a,b,c) = (a,b)(a,c) ; distributivité
(a,b)(b,c) = (c,b,a) ; relation de Charles
2. Quelle est l'inverse (réciproque) de (a,b,c) ?

Remarque : Soit à calculer (a,d)(a,b,c) on pose p = (a,d)(a,b,c) et on fait.
p(a) = a. (a,d)(a,b,c) = d.(a,b,c) = d
p(b) = b. (a,d)(a,b,c) = b.(a,b,c) = c
p(c) = c. (a,d)(a,b,c) = c.(a,b,c) = a
p(d) = d. (a,d)(a,b,c) = a.(a,b,c) = b
Les cycles sont comme les filtres on passe ou on change.

(a,d)(a,b,c) = (a,d,b,c)

4.1 SIGNATURE

Permutation paire, impaire

On sait que toute permutation p est décomposable (non unique) en produit de transpositions (2-cycle). Soit t le nombre de transpositions dans la décomposition, on dit que p est pair si t est pair, impair si non.
Pour des raisons pratiques dans les calculs on note pair = 1 et impair = -1

Signature d'une permutation
Par définition la signature d'une permutation p est :
$sig(p) = (-1)^t$, où t est le nombre de transpositions dans la décomposition.

On définit la signature d'un k-cycle par:
Si (k-1) est pair, la signature de ce k-cycle est pair , impair sinon
par ex

sig(4-cycle) = 4-1 = 3 = impair.
sig(3-cycle) = 3-1 = 2 = pair.
sig(2-cycle) = 2-1 = 1 = impair.
sig(1-cycle) = sig(id) = 1-1 = 0 = pair.
etc ....

Propriétés:

1. $sig(pq) = sig(p) . sig(q)$
2. $sig(k\text{-cycle}) = (-1)^{k-1}$
3. $sig(p^{-1}) = [sig(p)]^{-1}$
4. $sig(id) = 1$

ex:
$p = (a,b)(a,c)(d,e) \Rightarrow sig(p) = (-1)^3 \Rightarrow sig(p) = -1$;
permutation impaire (on a 3 couples à permuter)
$q = (a,b,c) = sig(q) = (-1)^{3-1} = (-1)^2 = 1$; paire

L'ensemble des permutations paire sera noté: A_n, le nombre de permutations sera noté $|S_n|$ c'est le cardinal de S_n ou le nombre d'éléments de S_n. On a
$|S_n| = n!$ et
$|A_n| = n!/2$

Théorème 3 :
Les 3-cycle (a,b,c) engendre A_n

Démonstration :

Il suffit d'exprimer le produit de deux transpositions par les 3-cycles .

¤ non-disjoint: (a,b)(b,c) = (c,b,a)

¤ disjoint: (a,b)(c,d) = (a,b)(b,c)^2(c,d) = (a,b)(b,c)(b,c)(c,d)

= (c,b,a)(d,c,b)

Théorème 4 :

La famille 3-cycle { (a,b,x) avec x ≠ a,b } engendre A_n

4.2 LES COMMUTATEURS

Un commutateur est un truc comme ça : $aba^{-1}b^{-1}$ que l'on note [a,b] (lire crochet ab) , on va noter S_n' l'ensemble engendré par des commutateurs. On appelle S_n' la dérivée de S_n (rappel: S_n c'est l'ensemble des permutations à n objets)

S_n' = < [a,b] avec a,b ∈S_n > engendré par des commutateurs
ou encore:
S_n' = { x = [a,b][c,d][e,f]... avec a,b,c,d,e,f... ∈S_n } produit des commutateurs

Note : l'ensemble des commutateurs ne forme pas un groupe, car en général le produit de 2 commutateurs n'est pas un commutateur. C'est l'ensemble des produits de commutateurs qui est un groupe.

Les permutations paires A_n forment un sous groupe de S_n .
On veut montrer que:
S_n' = A_n
Allons y ...

* $S'_n \subset A_n$

On a $[S_n:A_n] = 2$ ça signifie que S_n/A_n n'a que 2 éléments (2 classes) qui sont A_n et son complémentaire $\overline{A}_n$
Or A_n est l'élément neutre "1" de S_n/A_n d'où

$\overline{A}_n.1 = 1.\overline{A}_n$ donc S_n/A_n est commutatif.

Maintenant soit [a,b] et supposons que $[a,b] \in \overline{A}_n$
$[a,b] = aba^{-1}b^{-1} = k$ avec $k \in \overline{A}_n$
$aba^{-1}b^{-1} = k$
En passant par les classes, on a:
$A_na \,.\, A_nb \,.\, A_na^{-1} \,.\, A_nb^{-1} = A_nk$
$A_na \,.\, A_nb \,.\, A_na^{-1} \,.\, A_nb^{-1} \neq 1$ puisque $k \in \overline{A}_n$
$A_na \,.\, A_nb \,.\, A_na^{-1} \,.\, (A_nb)^{-1} \,.\, A_nb \neq A_nb$
$A_na \,.\, A_nb \,.\, A_na^{-1} \neq A_nb$
$A_na \,.\, A_nb \neq A_nb \,.\, A_na$
ce qui contredit S_n/A_n est commutatif donc $[a,b] \in A_n$

// Il y a une autre façon assez simple de montrer que $[a,b] \in A_n$, en effet
$[a,b] = aba^{-1}b^{-1}$
$sig([ab]) = sig(aba^{-1}b^{-1}) = sig(a)\, sig(b)\, [sig(a)]^{-1}[sig(b)]^{-1}$
$sig([ab]) = (-1)^t(-1)^m(-1)^{-t}(-1)^{-m} = 1.1 = 1$ //

Un commutateur [a,b] est dans A_n , donc le produit des commutateurs est dans A_n
Finalement
$S'_n \subset A_n$

* $A_n \subset S'_n$

Il suffit de remarquer qu'on a la formule suivante:
$(a,b,c) = (c,b,a)(a,c)(c,b,a)^{-1}\ (a,c)^{-1}$
un 3-cycle (a,b,c) s'exprime en commutateur et comme les 3-cycles engendrent A_n les éléments de A_n s'exprimeront en commutateurs c'est-à-dire on a:
$A_n \subset S_n'$
et finalement
$A_n = S_n'$

Autrement dit les permutations paires sont engendrées par les produits des commutateurs.

5 LE RUBIK'S CUBE

5.1 FIXER LE CUBE

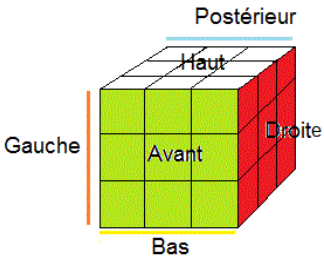
Tenez un Rubik's Cube (standard) en face de vous ou mieux encore posez le sur la table, le Cube possède alors 6 faces nommées ainsi dans cet ordre (nous verrons plus loin que cet ordre provient du marquage) :

H(aut) > B(as) > A(vant) > P(ostérieur) > G(auche) > D(roite).
En abrégeant :
H > B > A > P > G > D

Et pour nous les couleurs standards (dans cet ordre, l'ordre provient du marquage) seront :
b(lanc) > j(aune) > v(ert) > k(lein) > o(range) > r(ouge) .
En abrégeant :
b > j > v > k > o > r

Et ces couleurs seront associées aux faces de la façons suivantes:
H(aut) = b(lanc), B(as) = j(aune), A(vant) = v(ert), P(ostérieur) = k(lein), G(auche) = o(range), D(roite) = r(ouge) .

On dit qu'on a fixé, ou orienté le Cube.

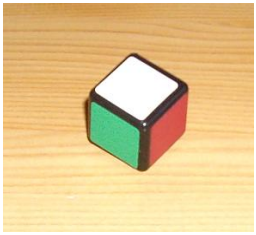


Nom des faces avec les couleurs standards

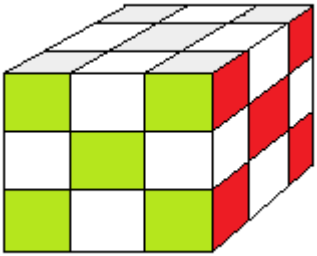
5.2 LES PIÈCES

La première chose à faire c'est de reconnaître les pièces . Si vous observez bien, vous verrez que le Rubik's Cube possède 3 sortes de pièces.

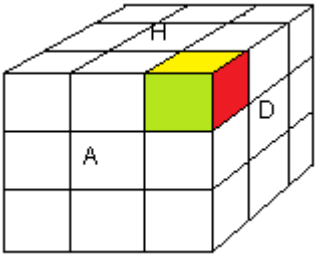
1. Les pièces portant 3 couleurs: les sommets, ce sont les coins du Cube. Il y a 8 sommets: 4 en Bas et 4 en Haut.



un sommet (une pièce)

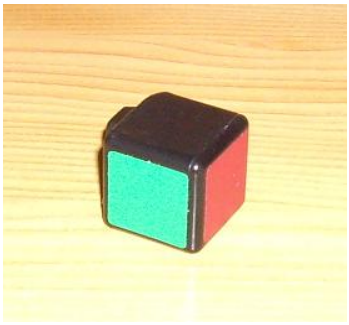


Les 8 sommets

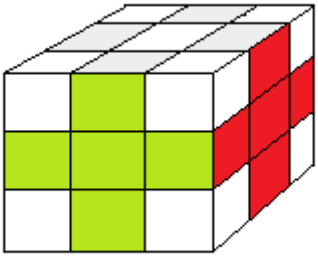


Un sommet avec ses 3 couleurs

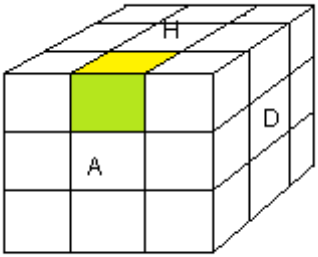
2. Les pièces portant 2 couleurs : les arêtes, elles se trouvent entre deux sommets. Il y a 12 arêtes : 4 en Bas, 4 en équateur et 4 en Haut



Une arête (une pièce)

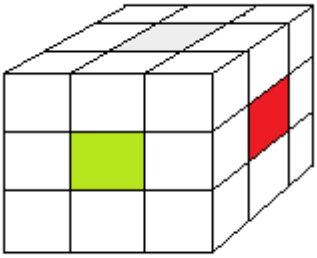


Les 12 arêtes

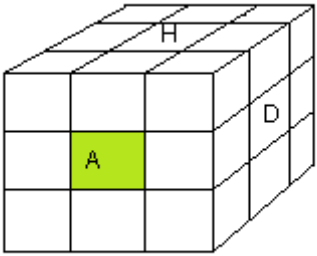


Une arête avec ses 2 couleurs

3. Les pièces portant une seule couleur : les centres, se trouvent au centre de la face, et il déterminent la couleur des faces: centre klein ⇒ face klein, centre rouge ⇒ face rouge etc ... Il y a 6 centres



Les 6 centres

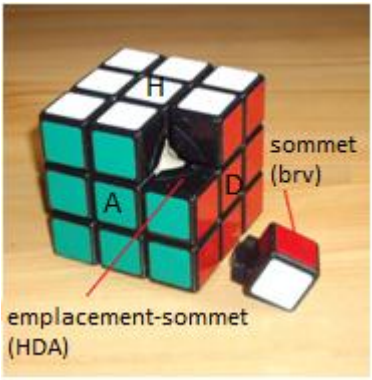


Un centre avec sa couleur

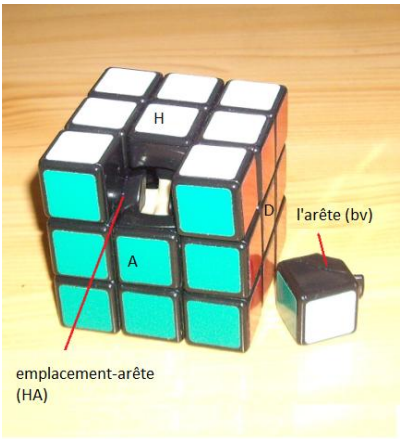
Les sommets, les arêtes, les centres, ces pièces restent dans leur camp, c'est-à-dire une arête reste toujours une arête elle ne devient jamais un centre ou un sommet, même chose pour les centres et les sommets. Toutes ces pièces sont distinctes (il y a 6+8+12 = 26) elles sont donc uniques. Pour le Rubik's Cube ce qui est important ce sont des arêtes et les sommets.
Lorsqu'on mélange le Cube les sommets et les arêtes bougent, mais aucun sommet ne se met à la place d'une arête et inversement, les sommets restent dans le clan des sommets les arêtes restent dans le clan des arêtes.

5.3 LES EMPLACEMENTS

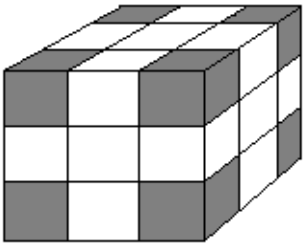
Il faut bien faire la distinction entre un emplacement (une position, un trou) et une pièce (arête, sommet, centre) : comme la maison et l'habitant. L'emplacement c'est la maison ; la pièce c'est l'habitant (l'habitant loge dans sa maison).



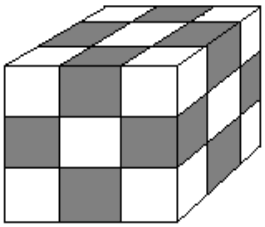
Emplacement et pièce



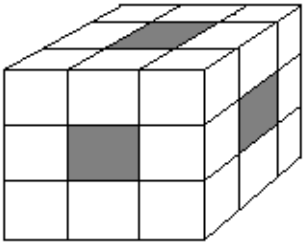
Emplacement et pièce



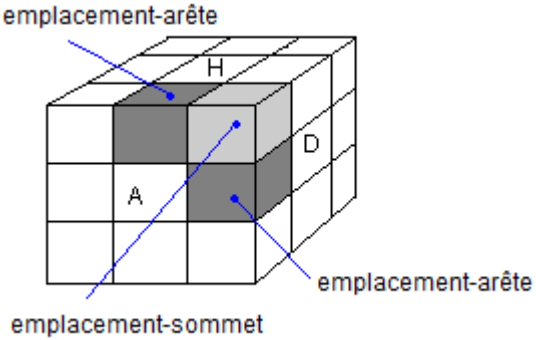
8 emplacements-sommets



12 emplacements-arêtes



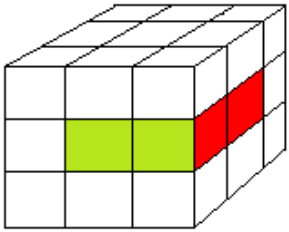
6 emplacements-centres



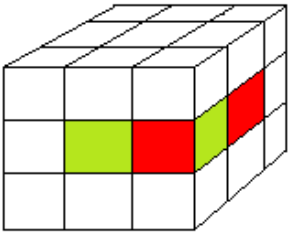
Chaque pièce du Rubik's Cube a un emplacement unique, son emplacement, il est repéré grâce aux centres.

6 SCHÉMA SOMMETS

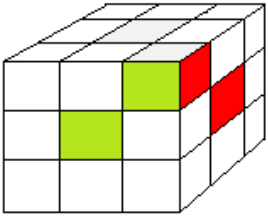
Lorsqu'on place une pièce dans son emplacement, elle peut être bien placée ou mal placée on dira qu'elle est bien orientée ou mal orientée. Bien orientée signifie que ses couleurs correspondent avec celle du centre



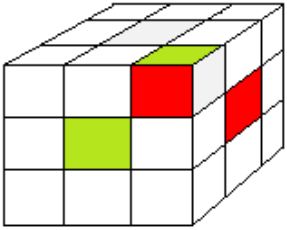
l'arête bien orientée



l'arête mal orienté

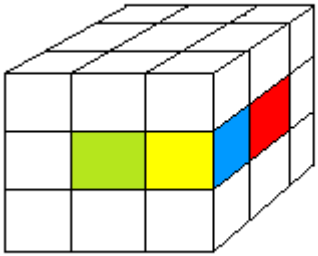


sommet bien orienté

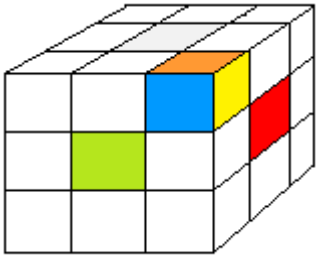


sommet mal orienté

Mais alors, comment savoir si une pièce est bien ou mal orientée quand elle est dans un autre emplacement que le sien ??



bien orientée ou mal orientée ?



bien orienté ou mal orienté ?

Pour répondre à cette question on doit passer par un système de marquage.

Il y a d'une part des emplacements-sommets à 3 facettes marquées 0, 1, -1 et d'autre part les sommets ayant 3 couleurs dont l'une est dominante. Lorsqu'un sommet se loge dans un emplacement-sommet et que sa couleur dominante est sur la facette marquée -1 on dit que l'orientation de ce sommet vaut -1, de même si sa couleur dominante est sur 1 son orientation vaut 1, sur 0 son orientation vaut 0 dans ce cas on dit que le sommet est bien orienté.

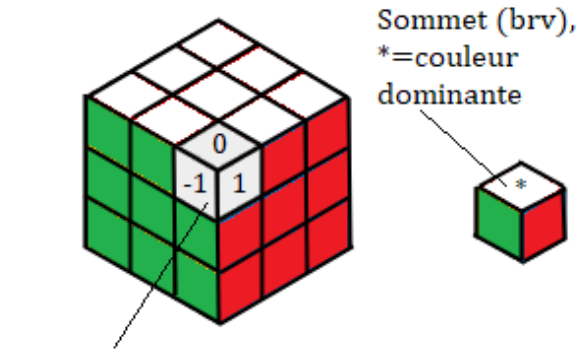
6.1 LE MARQUAGE DES FACETTES-SOMMETS

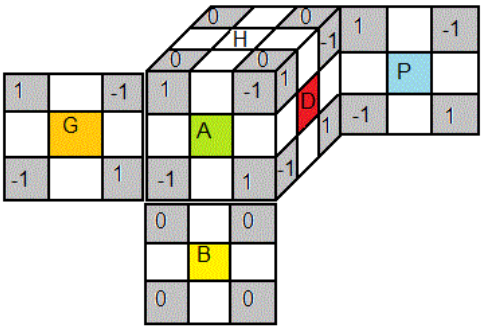
La grande question est : comment marquer ces facettes ??

Eh bien , examinons le problème de plus prés
Les sommets pivotent dans le sens horaire ou dans le sens contraire ce qui signifie que les autocollants des sommets doivent faire des cycles, par ex le sommet blanc-rouge-vert se place en Haut-Droite-Avant avec D = blanc alors on a nécessairement A = rouge et H = vert mais pas A = vert et H = rouge. Donc le marquage des facettes doit être "cyclique".

Il y a plusieurs façons de marquer mais ils sont tous équivalentes dans le sens qu'ils donnent tous les même lois du Rubik's Cube.
Nous décidons de marquer les facettes des sommets de la façon suivante : 0 sur le Haut et le Bas puis dans le sens

horaire 1, -1. Voici le diagramme de marquage des emplacements des sommets .





emplacements-sommets avec les facettes marquées dans le sens horaire
0 = bien orienté

Et ce qui donne l'ordre des faces :

H > B (les faces marquées zéro 0).

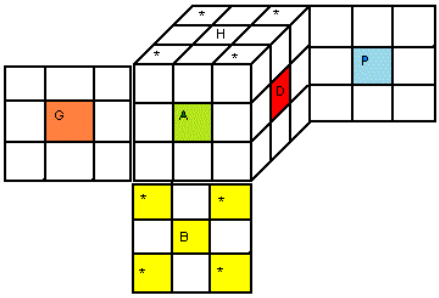
Un emplacement-sommet est un objet à facettes, il a un nom, l'initial des facettes qui le composent, et ils sont notés entre parenthèses .

Pour les noms de ces emplacements on utilise la règle : "face dominante + sens horaire"

Ce qui nous donne les 8 noms des emplacement-sommets dans cet ordre :
(HDA), (HAG), (HGP), (HPD)
(BAD), (BGA), (BPG), (BDP)

6.2 LA COULEUR DOMINANTE D'UN SOMMET

Pour un sommet, quelle est sa couleur dominante ? et pourquoi ?
Pour savoir la couleur dominante d'un sommet c'est très simple une fois le marquage est donné. A l'état résolu, la couleur dominante c'est la couleur qui est sur zéro 0. Parce que à l'état résolu tous les sommets sont en bonne orientation



* = les couleurs dominantes (* placé sur 0)

Et ce qui donne l'ordre des couleurs :

(b)lanc > (j)aune (couleur marquées zéro 0)

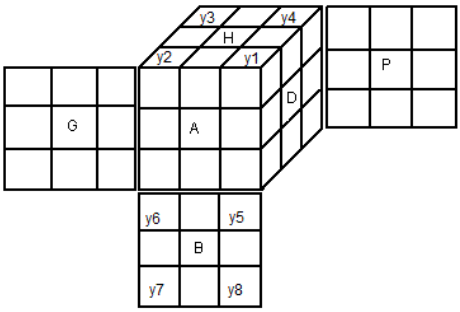
Un sommet est un objet à couleurs, il a un nom, l'initial des couleurs qui le composent, et ils sont notés entre parenthèses .

Pour les noms des sommets on utilise la règle :
"couleur dominante + sens horaire"
Ce qui nous donne les 8 noms des sommets, dans cet ordre:
(brv), (bvo), (bok), (bkr)
(jvr), (jov), (jko), (jrk)

6.3 NUMÉROTATION DES SOMMETS

On va numéroter les sommets (dans le sens horaire) en y_i comme indique la fig. ci-dessous
y_1 = (brv), y_2 = (bvo), y_3 = (bok), y_4 = (bkr),
y_5 = (jvr), y_6 = (jov), y_7 = (jko), y_8 = (jrk).

Remarque : on a placé les y_i sur la facette marquée 0



Les sommets numérotés: y_i

Au départ les emplacements-sommets contiennent les y_i comme suite:
(HDA) = y_1, (HAG) = y_2, (HGP) = y_3, (HPD) = y_4
(BAD) = y_5, (BGA) = y_6, (BPG) = y_7, (BDP) = y_8

6.4 L'ORIENTATION DES SOMMETS

Les sommets y_i se baladent pour se placer dans les emplacements-sommets, à chaque fois que la couleur dominante se trouve sur la facette marquée 1 son orientation vaut 1 (1 twist) , sur -1 son orientation vaut -1 (-1 twist) , sur 0 son orientation vaut zéro (0 twist, 0 = bien orienté). Par exemple, le sommet y_6 = (jov) se place en (HDA) avec jaune = A, alors y_6 vaut -1 (-1 twist) car la couleur dominante jaune est sur la facette -1, de même pour le sommet y_1 = (brv) dans (HAG) avec blanc = A, alors y_1=1 (1 twist) car la couleur dominante blanc se trouve sur 1 .

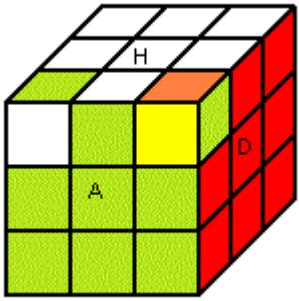


fig7

(6.4.1) La table des orientations des sommets

rotation	q=permutation	b=orientation
H	(1,2,3,4)	(0,0,0,0,0,0,0,0)
B	(5,8,7,6)	(0,0,0,0,0,0,0,0)
A	(1,5,6,2)	(-1,1,0,0,1,-1,0,0)
P	(4,3,7,8)	(0,0,-1,1,0,0,1,-1)
G	(3,2,6,7)	(0,-1,1,0,0,1,-1,0)
D	(1,4,8,5)	(1,0,0,-1,-1,0,0,1)

Note : 1) On voit que les rotations H, B ne changent pas l'orientation des sommets, seules les rotations A,P,G,D pivotent les sommets.

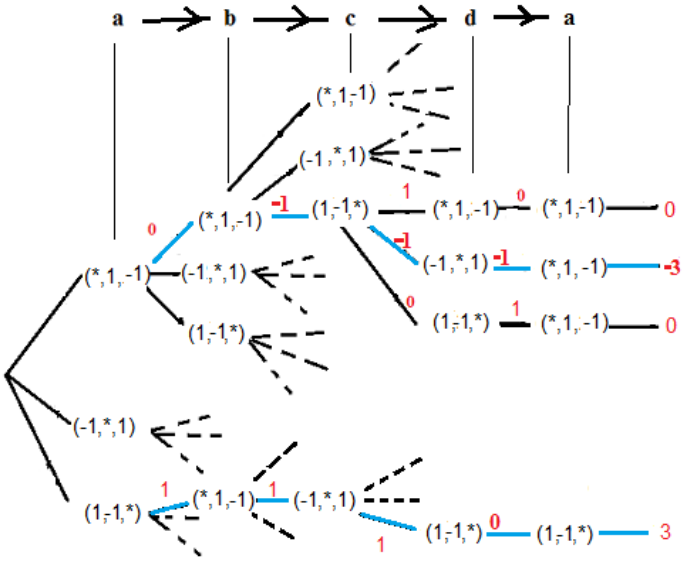
2) Si la couleur dominante tourne 1/3 tour dans le sens horaire ⇒ twist = 1, 1/3 tour dans le sens anti-horaire ⇒ twist = -1

6.5 L'ARBRE DE MARQUAGE DES EMPLACEMENTS-SOMMETS

Il y a plusieurs marquages possibles, mais ils sont tous équivalents (dans le sens où ils donnent les même lois du Rubik's Cube) , pour voir , il suffit de dessiner les arbres de marquages.

I. On a 2 types de marquages: horaire=(0,1,-1) et anti-horaire=(-1,1,0), donc 2 arbres
II. Lorsqu'on fait une rotation de base, il n'y a que 4 sommets disons a→b→c→d qui se déplacent, donc chaque'

arbre a 4 niveaux.
III. Chaque emplacement-sommet a 3 possibilités et on a 4 niveaux, l'arbre a $3^4 = 81$ branches
On va simplement dessiner une partie de l'arbre horaire.



* = les couleurs dominantes (* placé sur 0)

Voyons sur un chemin de l'arbre
a=(*,1,-1) → b=(*,1,-1) → c=(1,-1,*) → d=(-1,*,1) → a=(*,1,-1) ⇒ orientation = -3
on passe de a→b la couleur dominante '*' est sur 0
on passe de b→c la couleur dominante '*' est sur -1
on passe de c→d la couleur dominante '*' est sur -1
on passe de d→a la couleur dominante '*' est sur -1
total = -3

a=(1,-1,*) -› b=(*,1,-1) -› c=(-1,*,1) -› d=(1,-1,*) -› a=(1,-1,*) ⇒ orientation = 3
on passe de a-›b la couleur dominante '*' est sur 1
on passe de b-›c la couleur dominante '*' est sur 1
on passe de c-›d la couleur dominante '*' est sur 1
on passe de d-›a la couleur dominante '*' est sur 0
total = 3
etc ...

Il n'est pas difficile de calculer le nombre total des marquages possibles n. En effet un arbre a 81 branches, une branche représente le marquage de 4 emplacements-sommets comme on a 8 emplacements-sommets il nous faut 2 branches, càd il faut choisir 2 branches parmi 81, et on a 2 arbres donc
n = 2 x $\binom{81}{2}$ = 81 x 80 = 6480

L'arbre de marquage des emplacements-sommets nous montre qu'une rotation de base, apporte 0 ou 3 ou -3 au nombre de twists

7 SCHÉMA ARÊTES

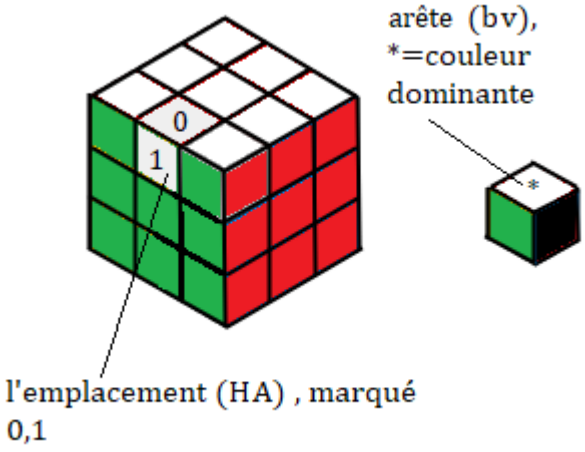
Comme pour les sommets, on a d'une part, des emplacements-arêtes à 2 facettes marquées 0, 1 et d'autre part des arêtes ayant 2 couleurs dont l'une est dominante. Lorsqu'une arête se loge dans un emplacement-arête et que sa couleur dominante est sur 1 on dit que l'orientation de cette arête vaut 1, de même si sa couleur dominante est sur 0 son orientation vaut 0 on dit dans ce cas qu'elle est bien orientée.

7.1 LE MARQUAGE DES FACETTES-ARÊTES

Le marquage des facettes est 0, ou 1, car les arêtes n'ont que 2 possibilités pour renverser .

On marque 0 sur une facette, puis on marque 1 pour l'autre facette.

Nous décidons de marquer les facettes des arêtes comme indique la fig. ci-dessous: 0 sur H, B puis 0 sur A et P, voici le diagramme de marquage des emplacements des arêtes .



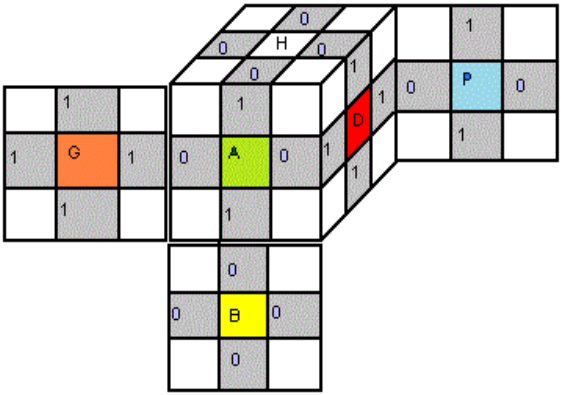


fig1

emplacements-arêtes avec les facettes marquées
0=bien orienté

Et ce qui donne l'ordre des faces:

H > B > A > P > G > D (les faces marquées zéro 0).

Un emplacement-arête est un objet à facettes, il a un nom, l'initial des facettes qui le composent, et ils sont notés entre parenthèses .

Pour les noms de ces emplacements on utilise la règle :

"face dominante"

Voici les 12 noms des emplacements-arêtes dans cet ordre (ici on n'a pas besoin "sens horaire")
(HA), (HG), (HP), (HD)
(AD), (AG), (PG), (PD)
(BA), (BG), (BP), (BD)

7.2 LA COULEUR DOMINANTE D'UNE ARÊTE

Pour une arête, quelle est sa couleur dominante ? et pourquoi ?
Une fois le marquage est donné, à l'état résolu, la couleur dominante c'est la couleur qui est sur zéro 0. Parce que à

l'état résolu tous les arêtes sont en bonne orientation

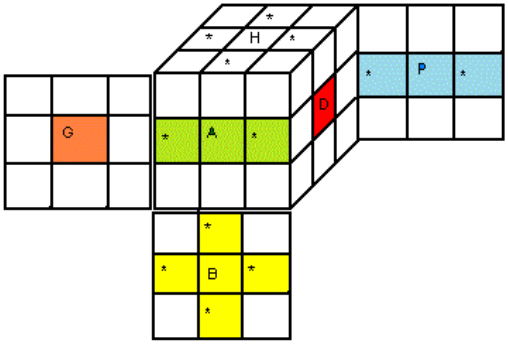


fig3

* = les couleurs dominantes (* placé sur 0)

Et ce qui donne l'ordre des couleurs:
b(lanc) > j(aune) > v(ert) > k(lein) > o(range) > r(ouge) ;
(les couleurs marquées zéro 0)

Une arête est un objet à couleurs, elle a un nom, l'initial des couleurs qui la composent, et elles sont notées entre parenthèses .

Pour les noms des arêtes on utilise la règle :

"couleur dominante"

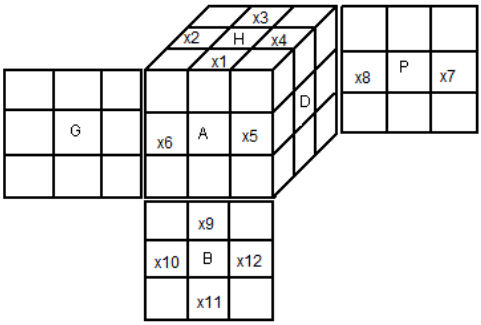
Voici les 12 noms des arêtes dans cet ordre :

(bv), (bo), (bk), (br)
(vr), (vo), (ko), (kr)
(jv), (jo), (jk), (jr)

7.3 NUMÉROTATION DES ARÊTES

On va numéroter les arêtes (dans le sens horaire) en x_i comme indique la fig. ci-dessous
x_1=(bv), x_2=(bo), x_3=(bk), x_4=(br),
x_5=(vr), x_6=(vo), x_7=(ko), x_8=(kr),
x_9=(jv), x_{10}=(jo), x_{11}=(jk), x_{12}=(jr).

Remarque : on a placé les x_i sur la facette marquée 0



Les arêtes numérotés: x_i

Au départ les emplacements contiennent les x_i comme suite:
(HA)=x_1, (HG)=x_2, (HP)=x_3, (HD)=x_4
(AD)=x_5, (AG)=x_6, (PG)=x_7, (PD)=x_8
(BA)=x_9, (BG)=x_{10}, (BP)=x_{11}, (BD)=x_{12}

7.4 L' ORIENTATION DES ARÊTES

Les arêtes x_i se baladent d'emplacements en emplacements pour se loger dans des emplacements-arêtes (HA), (HD)..., à chaque fois que la couleur dominante se trouve sur la facette marquée 1 sa orientation vaut 1 (1 flip), sinon elle vaut zéro (0=bien orienté), Par exemple l'arête (vr)=x_5 se place en (HA) avec vert=H, alors x_5 vaut 0 (0 flip, bien orienté) car la couleur dominante vert est sur la facette marquée 0, De même, si l'arête (bk)=x_3 est dans (AD) avec blanc=D, alors x_3 = 1 (1 flip) car la couleur dominante blanc se trouve sur 1

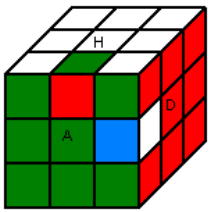


fig4

(7.4.1) La table des orientations des arêtes

rotation	p=permutation	a=orientation
H	(1,2,3,4)	(0,0,0,0,0,0,0,0,0,0,0,0)
B	(9,12,11,10)	(0,0,0,0,0,0,0,0,0,0,0,0)
A	(1,5,9,6)	(1,0,0,0,1,1,0,0,1,0,0,0)
P	(3,7,11,8)	(0,0,1,0,0,0,1,1,0,0,1,0)
G	(2,6,10,7)	(0,0,0,0,0,0,0,0,0,0,0,0)
D	(4,8,12,5)	(0,0,0,0,0,0,0,0,0,0,0,0)

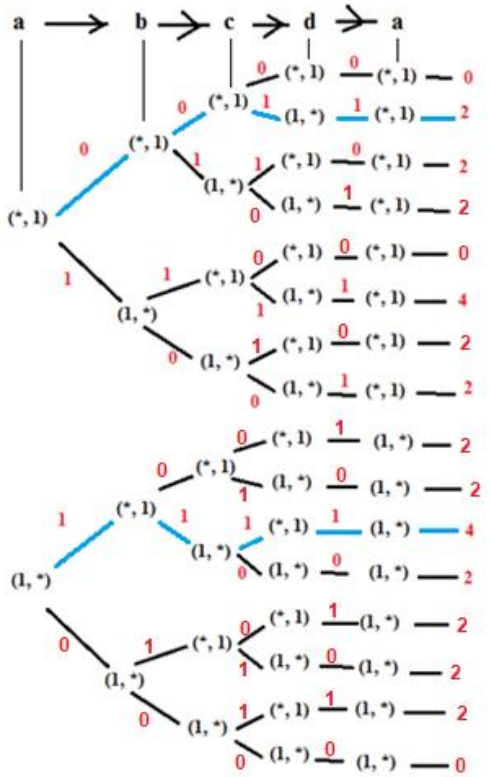
Note : 1) On voit que les rotations H,B,G,D ne changent pas l'orientation des arêtes, seules les rotations A et P pivotent les arêtes.

2) Si la couleur dominante est sur la facette 0 ⇒ flip=0, sur la facette 1 ⇒ flip=1

7.5 L'ARBRE DE MARQUAGE DES EMPLACEMENTS-ARÊTES

Il y a plusieurs marquages possibles mais ils sont tous équivalents (dans le sens qu'ils donnent les même lois du Rubik's Cube) pour voir dessinons l'arbre de marquage des emplacements-arêtes. Lorsqu'on fait une rotation de

base, il n'y a que 4 arêtes disons a→b→c→d qui se déplacent, l'arbre a donc 4 niveaux, comme chaque emplacement-arête a 2 possibilités et on a 4 niveaux donc l'arbre a $2^4 = 16$ branches.



* = les couleurs dominantes (* placé sur 0)

Voyons sur un chemin de l'arbre
a=(*,1) -→ b=(*,1) -→ c=(*,1) -→ d=(1,*) -→ a=(*,1) ⇒
orientation = 2
on passe de a-→b la couleur dominante '*' est sur 0
on passe de b-→c la couleur dominante '*' est sur 0
on passe de c-→d la couleur dominante '*' est sur 1
on passe de d-→a la couleur dominante '*' est sur 1
total = 2

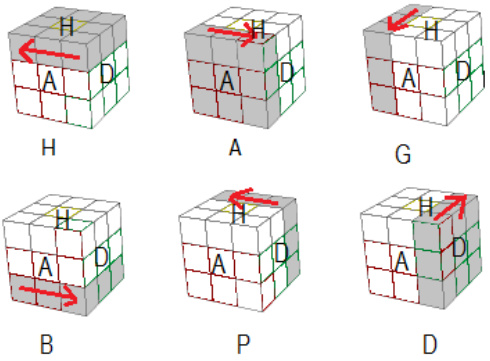
a=(1,*) -→ b=(*,1) -→ c=(1,*) -→ d=(*,1) -→ a=(1,*) ⇒
orientation = 4
on passe de a-→b la couleur dominante '*' est sur 1
on passe de b-→c la couleur dominante '*' est sur 1
on passe de c-→d la couleur dominante '*' est sur 1
on passe de d-→a la couleur dominante '*' est sur 1
total = 4
etc ...

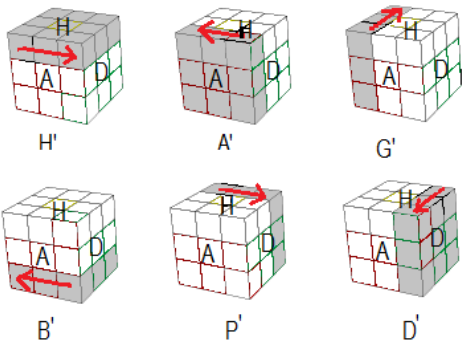
De même on va calculer le nombre total des marquages possibles n. l'arbre a 16 branches, il faut choisir 3 branches (3x4=12 arêtes) parmi 16
n = $\binom{16}{3}$ = 16x15x14/3! = 560

L'arbre de marquage nous montre qu'une rotation de base, apporte 0 ou 2 ou 4 au nombre de flips

8 LES ROTATIONS

Les rotations de base : { H, B, A, P, G, D }
A = On se place devant la face Avant et on tourne 90° la face Avant dans le sens des aiguilles d'une montre (sens horaire).
A' = A^{-1} = On se place devant la face Avant et on tourne -90° la face Avant (sens anti-horaire), on dit que A' est l'inverse de A.
A^2 = AA = On se place devant la face Avant et on tourne la face Avant 180° .



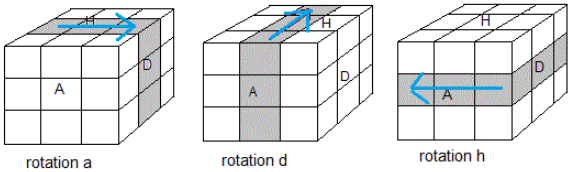


Rotations tranches : {h, d, a}

a = On se place devant la face Avant et on tourne 90° la tranche avant-intérieur (tranche a) dans le sens horaire.

a' = a^{-1} = On se place devant la face Avant et on tourne -90° la tranche avant-intérieur (sens anti-horaire) .

a^2 = aa = On se place devant la face Avant et on tourne 180° la tranche avant-intérieur.

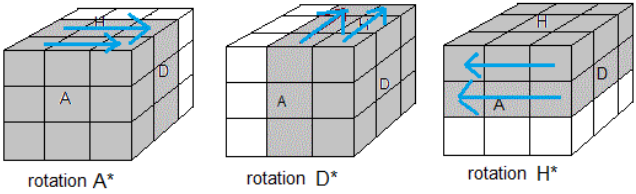


Rotations bloc : {H*, D*, A*}

A* = On se place devant la face Avant et on tourne le bloc (aA) 90° dans le sens des aiguilles d'une montre.

A*' = On se place devant la face Avant et on tourne le bloc (aA) -90° (sens anti-horaire).

A^{*2} = A*A* = On se place devant la face Avant et on tourne le bloc (aA) 180° .

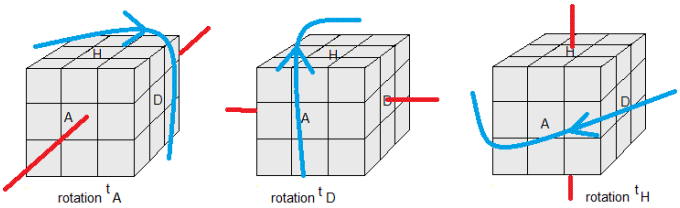


Rotation cube : { ${}^{t}H$, ${}^{t}D$, ${}^{t}A$ }

${}^{t}A$ = On se place devant la face Avant et on tourne le Cube entier 90° dans le sens horaire.

${}^{t}A'$ = On se place devant la face Avant et on tourne le Cube entier -90° (sens anti-horaire) .

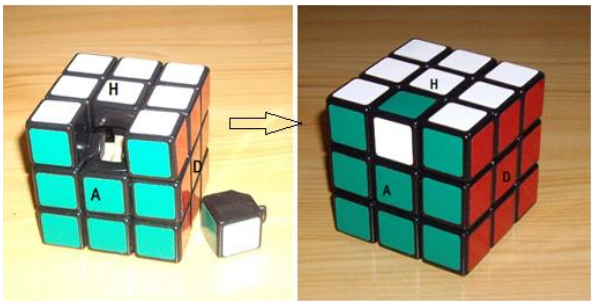
${}^{t}A^{2}$ = On se place devant la face Avant et on tourne le Cube entier 180° .



Rotations étendues : {Γ, ψ, Ω}

Rotation étendue Γ : Inverser l'arête (HA)[2]

1. On enlève l'arête (HA)
2. La pivote 180°
3. Puis on la remet



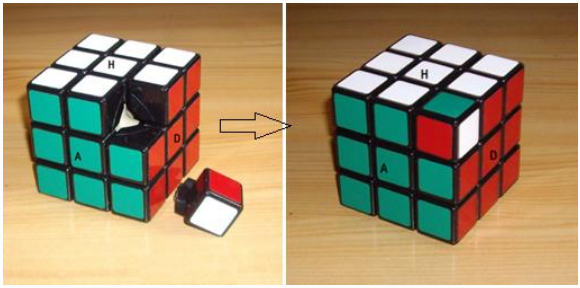
Rotation étendue Γ = $(HA)^{-}$

[2] Par abuse de langage on dit l'arête (HA) au lieu de l'arête contenue dans (HA).

Par définition ce manœuvre se nomme rotation étendue Γ qui a comme résultat , l'arête (HA) est pivotée 180°
$(HA)^{-} = \Gamma$

<u>Rotation étendue</u> ψ : Pivoter le sommet (HDA)[3]

1. On enlève le sommet (HDA)
2. Le pivote 120° dans le sens horaire
3. Puis on le remet



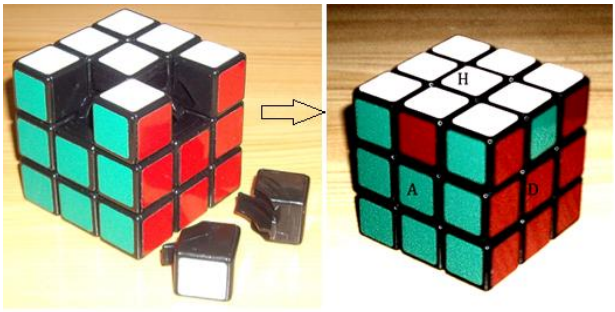
Rotation étendue $\psi = (HDA)^{+}$

Ce manœuvre , par définition , se nomme rotation étendue ψ qui a comme résultat, le sommet (HDA) pivoté 120° dans le sens horaire
$(HDA)^{+} = \psi$

[3] Par abuse de langage on dit le sommet (HDA) au lieu de le sommet contenu dans (HDA).

Rotation étendue Ω : Permuter deux arêtes (HA), (HD)

1. On enlève les arêtes (HA), (HD)
2. Permute (HA)↔(HD)
3. Puis on les remet



Rotation étendue Ω = (HA)↔(HD)

Ce manœuvre , par définition , se nomme rotation étendue Ω qui a comme résultat, les arêtes (HA) , (HD) sont permutées
(HA)↔(HD) = Ω

Les rotations étendues ce sont des rotations qui violent les lois.

8.1 FORMULES

Une autre notion très importantes à comprendre: la notion de formule (= mouvement, = mélange, = manœuvre),

Définition une formule :

On note :
M = < H, B, A, P, G, D >

On dit que M est engendré par les rotations de base.

Une formule est donc une suite finie de rotations de base {H,B,A,P,G,D} (et leur inverse bien sûr) avec la règle :

* On convient d'éviter de faire HH', H'H, BB', B'B, AA', A'A etc ... dans une formule.

par ex:

$AHB'P^2DG'$; ok

$GBHH'D^2BP$; interdit: car HH'

HDH'D' ; ok

et on pose

HH' = H'H = BB'= B'B = AA' = A'A = ... = I

I se nomme formule neutre (on ne fait rien)

Par définition I est une formule

Une rotation de base ou leur inverse est donc une formule.

$D^2GB'dHD'PA$, $DA^tHG'D^2$ ne sont pas des formules proprement parler car elles contiennent d et ^tH qui ne

sont pas des rotations de bases , mais dans la pratique on parle quand même des formules.

Remarque : à ce stage M est infini, en effet on peut avoir :

A, AAA, AAAAAA, AAAAAAAAA, ...

8.2 FORMULES ÉTENDUES

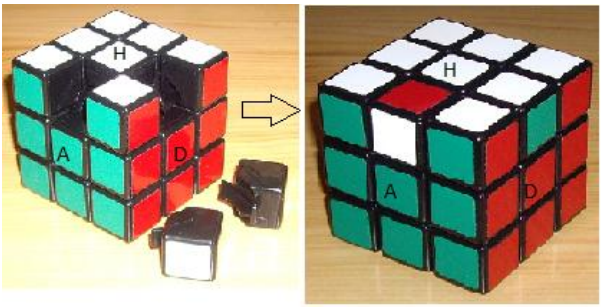
On note :
$M^+ = < H, B, A, P, G, D , \Gamma, \psi, \Omega >$

M^+ est donc engendré par les 6 rotations de base et les 3 rotations étendues.
Une formule étendue est donc une suite finie de rotations contenant au moins une rotation étendue, du genre $AH\Gamma P\Omega' B\psi^2$ ...

Là aussi , dans une formule étendue , il est interdit de faire AA', A'A , ΓΓ', Γ'Γ, ...

Une rotation étendue est donc une formule étendue par ex la rotation étendue Γ.

Voici un ex d'une formule étendue ΩΓ:
1. On enlève les arêtes (HA), (HD)
2. Permute (HA)↔(HD)
3. Pivote (HA)
4. Puis on les remet



formule étendue $\Omega\Gamma = (HA)^{-} \leftrightarrow (HD)$

$(HA^{-}, HD) = \Omega\Gamma$

NOTE : Là aussi on a M^{+} est infini

8.3 LONGUEUR D'UNE FORMULE

La longueur d'une formule V[4] c'est le nombre de rotations qu'elle contient et on la note |V| , par ex:

$|I| = 0$ il n'y a aucune rotation dans I

$|A| = 1$, $|A'|=1$, $|A^2| = 2$,

$S = AD^3A'D'H^2P'^2$, $V = \Gamma^2\Omega D^3GA'$

$|S| = 10$, $|V| = 8$

---

[4] On suppose toujours que V est une écriture minimale. En fait la longueur est définie par |V| = longueur de l'écriture minimale

On dit qu'on a utilisé la métrique "quart" , (q-rotation)

On rencontre dans la littérature du Rubik's Cube une autre façon de compter la longueur , on compte $|A^2| = 1$ on dit dans ce cas on utilise le métrique "face" (f-rotation) et on le précise avec un 'f'.

$|I| = 0f$

$|A| = 1f$, $|A'|=1f$, $|A^2| = 1f$,
$S = AD^3A'D'H^2P'^2$, $V = \Gamma^2\Omega D^3GA'$
$|S| = 7f$, $|V| = 6f$
Pour nous on utilise toujours la métrique "quart".

9 LE GROUPE DES FORMULES (M, .)

L'ensemble des formules M muni le produit (la concaténation) de deux formules forme un groupe (M, .) , en effet on a:

1. Le produit VT (on fait V puis T) d'une formule V par une formule T, est encore une formule (loi interne).
2. La formule I consiste à rien faire, on l'appelle formule neutre (élément neutre).

   VI = IV = V

3. Chaque formule V a un inverse V' (noté aussi parfois V^{-1}): VV' = V'V = I (symétrique)

   V = AB'H'DP ⇒ V' = P'D'HBA'

4. Faire (VT) puis S c'est la même chose que faire V puis (TS):
   (VT)S = V(TS) (associative)

(M, .) est donc un groupe , le groupe des formules du Rubik's Cube.

On fait la même chose avec M^+ , donc (M^+, .) est aussi un groupe, le groupe des formules étendues du Rubik's Cube .

On a évidemment M est un sous groupe de M^+.

Mais ce n'est ni M ni M^+ ce sera ce qu'on appelle le groupe du Rubik's Cube !, contrairement à beaucoup de gens y croient .
(M^+, .) est donc le groupe des formules étendues du Rubik's Cube , et (M, .) le groupe des formules du Rubik's Cube.

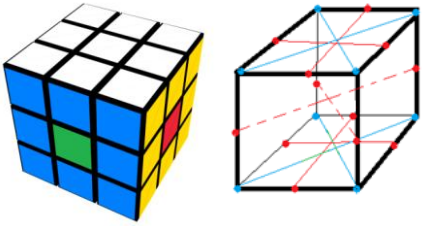
Formules célèbres
M = < H,B,A,P,G,D >

* On peut avoir 5 générateurs
M = < H,A,P,G,D > où B = $(DG'A^2P^2DG')H(DG'A^2P^2DG')$ (Roger Penrose)

* On peut avoir 2 générateurs
M = < T,K > où T = HPGHG'H'P' et K = $D^2AGB'D'$ (Frank Barnes)

* $DH^2B'PB'$, cette formule possède l'ordre maximal 1260
$(DH^2B'PB')^{1260} = I$

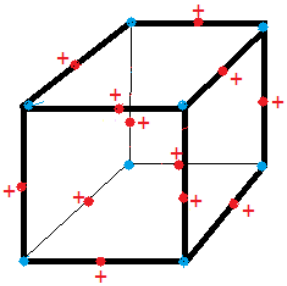
* 4Spot Ω :
Ω = (face A, face P)(face G, face D)
4Spot = Ω = $BP^2A^2BH'G^2D^2H'$ (12*) ;
|Ω| = 12* (*=minimal)



4Spot

* <u>SuperFlip Φ (12 arêtes flippées)</u> :
$\Phi = (HA)^+(HP)^+(HG)^+(HD)^+(AD)^+(PG)^+(AG)^+(PD)^+(BA)^+(BP)^+(BG)^+(BD)^+$

$\Phi = D'H^2PG'\ .AH'PBA\ .HB'GB^2\ .A'DP'BA'\ .H'P'HB'$ (Michael Reid ,1995, par ordinateur)
$|\Phi| = 24$ (24* minimal, Jerry Bryan, 1995)



SuperFlip

* 12 arêtes flippées

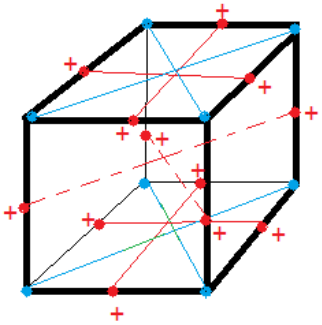
* <u>SuperFlip4Spot Π</u> :
$\Pi = H^2B^2G\ A^2\ .H'BD^2\ PH'B'D.\ GA^2D\ HB'\ D'GHA'P'$ (Mike Reid, par ordinateur)

|Π| = 26 (26* minimal Mike Reid)

Π = A DG'PB .A D'HBP .D' B'D'PH² .B²P²DGB²DG
|Π| = 26

Π = H²AH²D' .G A²HA' .P'DGH² .DHB'DG' .BD'G'B²
|Π| = 26

Π = (HA⁺,HP⁺)(HG⁺,HD⁺) (AD⁺,PG⁺)(AG⁺,PD⁺)
(BA⁺,BP⁺)(BG⁺,BD⁺)(HDA,HGP)(HAG,HPD)(BAD,BPG)
(BGA,BPD)

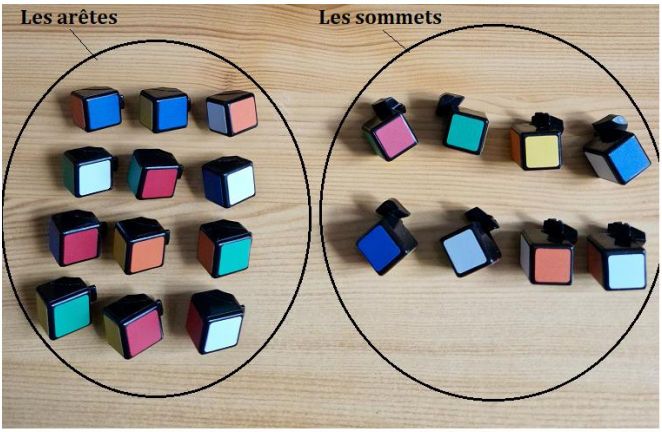


SuperFlip4Spot

* 4 couples sommets-opposés sont échangés
* 6 couples arêtes-opposées sont échangés
* Toutes les arêtes sont flippées
On l'appelle SuperFlip4Spot car c'est le produit de SuperFlip et 4Spot.
Π = ΦΩ = ΩΦ

10 LE GROUPE DES CONFIGURATIONS (G^+, .)

On imagine donc le Rubik's Cube n'a pas de core, les arêtes et les sommets bougent librement mais restent dans leur camp (c'est normal, car physiquement ces pièces sont différentes).



$G^+ = S_{12} \times \mathbb{Z}_2{}^{12} \times S_8 \times \mathbb{Z}_3{}^8$

1) Dans G^+ on peut permuter les sommets entre eux sans toucher les autres pièces.

2) Dans G^+ on peut pivoter un sommet sans toucher les autres pièces.

4) Dans G^+ on peut permuter les arêtes entre elles sans toucher les autres pièces.

5) Dans G^+ on peut pivoter une arête sans toucher les autres pièces.

*On peut permuter ces 12 arêtes entre elles comme on veut, on a affaire à S_{12} (le groupe des permutations à 12 objets) et chaque arête possède 2 orientations, on a donc affaire à $\mathbb{Z}_2^{12}$, finalement pour les arêtes on a :

$S_{12} \times \mathbb{Z}_2^{12}$

*De même pour les sommets, on peut permuter ces 8 sommets entre eux comme on veut, on a affaire à S_8 et chaque sommet possède 3 orientations, on a donc affaire à $\mathbb{Z}_3^8$, pour les sommets on a :

$S_8 \times \mathbb{Z}_3^8$

finalement on pose:

$G^+ = S_{12} \times \mathbb{Z}_2^{12} \times S_8 \times \mathbb{Z}_3^8$

$\mu = (u, x, v, y)$ $u \in S_{12}$, $x \in \mathbb{Z}_2^{12}$, $v \in S_8$, $y \in \mathbb{Z}_3^8$

G^+ se nomme l'ensemble des configurations .

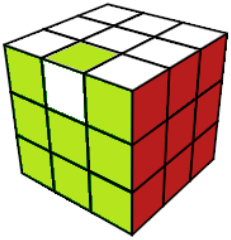
$|G^+| = 12! .2^{12} \times 8! .3^8$

S_{12} = Le groupe des permutations des arêtes
$\mathbb{Z}_2^{12}$ = Le groupe des orientations des arêtes
S_8 = Le groupe des permutations des sommets
$\mathbb{Z}_3^8$ = Le groupe des orientations des sommets

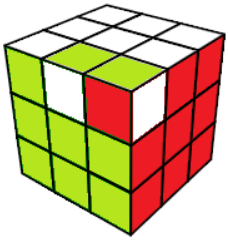
Remarque :
Pour connaître une configuration μ, il suffit de poser les 4 questions suivantes:
1) où se trouvent les 12 arêtes ? ==> S_{12}
2) comment les 12 arêtes sont-elles orientées ? ==> $\mathbb{Z}_2{}^{12}$
3) où se trouvent les 8 sommets ? ==> S_8
4) comment les 8 sommets sont-ils orientés ? ==> $\mathbb{Z}_3{}^8$

$\mu = (u, x, v, y)$ $u \in S_{12}$, $x \in \mathbb{Z}_2{}^{12}$, $v \in S_8$, $y \in \mathbb{Z}_3{}^8$

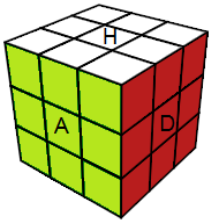
Voici la visualisation des configurations



une configuration



une autre configuration



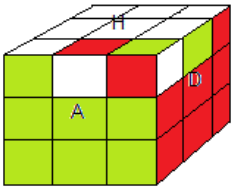
e=configuration résolue, une couleur par face.

On peut voir que les centres ne sont pas bougés :
Haut=blanc, Avant=vert, Droite=rouge, ...

L'orientation du Cube reste intacte.
Une configuration respecte l'orientation du Cube, càd on mélange le Cube avec les rotations de base et étendus sans bouger, ni tourner le Cube, c'est comme s'il y a un mécanisme qui fixe le Cube et on peut seulement tourner les faces.

Une autre façon de voir G^+ : On démonte le Cube et on remonte le Cube au hasard , on tient le Cube de telle sorte que :
H(aut) = b(lanc), B(as) = j(aune), A(vant) = v(ert), P(ostérieur) = k(lein), G(auche) = o(range), D(roite) = r(ouge) .

Le motif obtenu est une configuration , càd un élément de G^+ , voici 2 ex



une configuration

une autre configuration

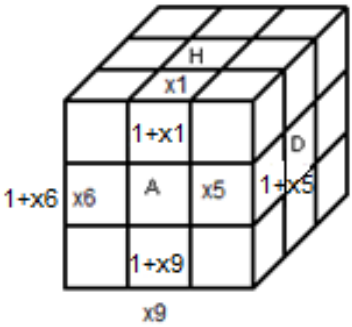
11 LOI DE COMPOSITION DANS $(G^+,.)$

On veut définir une loi '.' dans G^+ .

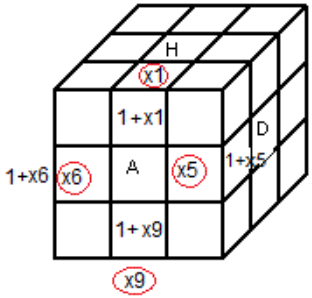
Lorsqu'on applique une rotation de base (sur la configuration résolue) , A par ex on voit que les pièces se déplacent et pivotent.

Soit donc (p,a,q,b) la configuration associée à la rotation A: $A \rightarrow (p,a,q,b)$

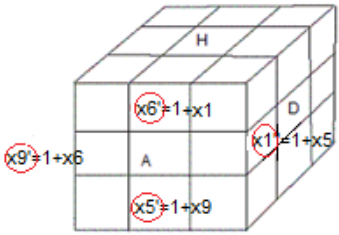
I) <u>Pour les arêtes</u> : La rotation de base A génère une permutation p et une orientation a : $A \rightarrow (p,a)$.
D'après le marquage on a:
$(HA) = (x_1,1+x_1)$, $(AD) = (x_5,1+x_5)$, $(BA) = (x_9,1+x_9)$, $(AG) = (x_6,1+x_6)$



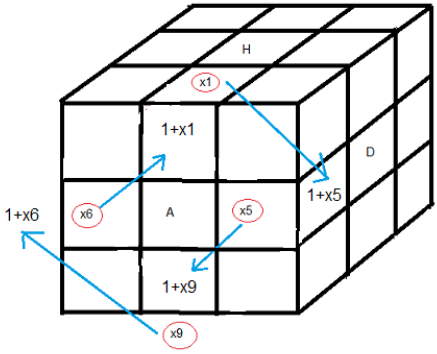
Numérotation des arêtes



Avant la rotation A



Après la rotation A



$x'_1 = 1+x_5$
$x'_2 = x_2$
$x'_3 = x_3$
$x'_4 = x_4$
$x'_5 = 1+x_9$
$x'_6 = 1+x_1$
$x'_7 = x_7$
$x'_8 = x_8$
$x'_9 = 1+x_6$
$x'_{10} = x_{10}$
$x'_{11} = x_{11}$
$x'_{12} = x_{12}$

Or pour la rotation A on a :
Permutation: p = (1,5,9,6)
Orientation: a = (1,0,0,0,1,1,0,0,1,0,0,0)
d'où:
x' = a + p(x)
où $p(x) = (x_{p(1)}, x_{p(2)}, x_{p(3)},..., x_{p(12)})$; permutation des x_i par p

Une formule T≠I (et la configuration associée (u',x')) commence toujours par une rotation de base par ex A (la configuration associée (p,a)) et le reste V (la configuration associée (u,x)) on a donc :

T = AV

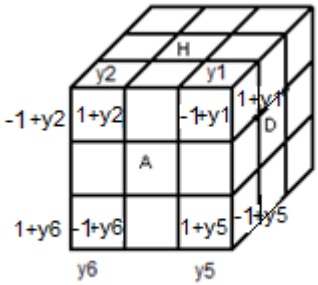
(u',x') = (p,a)(u,x) = (pu, a+p(x))

ce qui suggère que la loi dans $(G^+, .)$ vaut (pour les arêtes):
(u,x)(u',x') = (uu', x+u(x'))

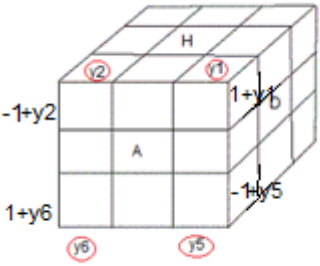
uu' = u' o u

où $u(x) = (x_{u(1)}, x_{u(2)}, x_{u(3)},.., x_{u(12)})$; permutation des x_i par u

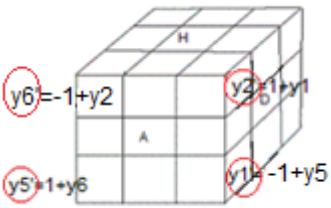
II) Pour les sommets : De même la rotation de base A génère une permutation q et une orientation b: $A \rightarrow (q,b)$.
D'après le marquage on a:
$(HAG) = (y_2, 1+y_2, -1+y_2)$, $(HDA) = (y_1, 1+y_1, -1+y_1)$,
$(BGA) = (y_6, 1+y_6, -1+y_6)$, $(BAD) = (y_5, 1+y_5, -1+y_5)$.



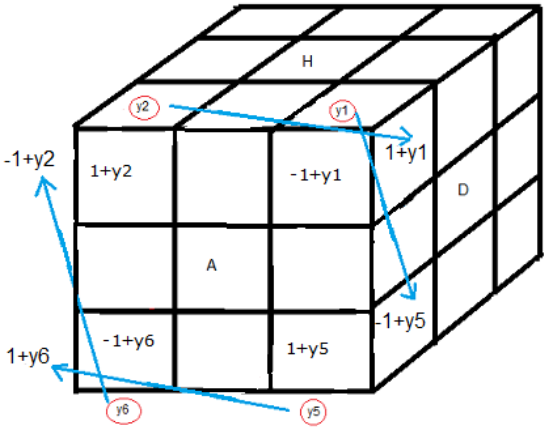
Numérotation des sommets



Avant la rotation A



Après la rotation A



$y'_1 = -1+y_5$
$y'_2 = 1+y_1$
$y'_3 = y_3$
$y'_4 = y_4$
$y'_5 = 1+y_6$
$y'_6 = -1+y_2$
$y'_7 = y_7$
$y'_8 = y_8$

or pour la rotation A on a :
Permutation: q = (1,5,6,2)
Orientation: b = (-1,1,0,0,1,-1,0,0)
d'où :
y' = b+q(y)
où $q(y) = (y_{q(1)}, y_{q(2)}, y_{q(3)},..., y_{q(8)})$

Une formule T≠I (et la configuration associée (v',y')) commence toujours par une rotation de base par ex A (la configuration associée (q,b)) et le reste V (la configuration associée (v,y)) on a donc :

T = AV

(v',y') = (q,b)(v,y) = (qv, b+q(y))

ce qui suggère que la loi dans $(G^+, .)$ vaut (pour les sommets):
(v,y)(v',y') = (vv', y+v(y'))

où $v(y) = (y_{v(1)}, y_{v(2)}, y_{v(3)},..., y_{v(8)})$

On va donc définir la loi dans G^+ comme suite:

$\mu,\mu' \in G^+$
$\mu = (u,x,v,y)$ et $\mu' = (u',x',v',y')$
$\mu\mu' = (u,x,v,y)(u',x',v',y') = (uu', x+u(x'), vv', y+v(y'))$

où

uu' = u' o u, vv' = v' o v

$u(x) = (x_{u(1)}, x_{u(2)}, x_{u(3)},..., x_{u(12)})$; permutation des x_i par u

$v(y) = (y_{v(1)}, y_{v(2)}, y_{v(3)},..., y_{v(8)})$; permutation des y_i par v

Voyons si cette loi confère à $(G^+, .)$ une structure de groupe.

1) $\mu,\mu' \in G^+ \Rightarrow \mu\mu' \in G^+$; c'est bien une loi interne

2) e = (id,0,id,0) élément neutre

$\mu e = (u,x,v,y)(id,0,id,0) = (u, x+u(0), v, y+v(0)) = (u,x,v,y)$

$e\mu = (id,0,id,0)\ (u,x,v,y) = (u, 0+id(x), v, 0+id(y)) = (u,x,v,y)$

3) $\mu^{-1} = (u^{-1}, u^{-1}(-x))$

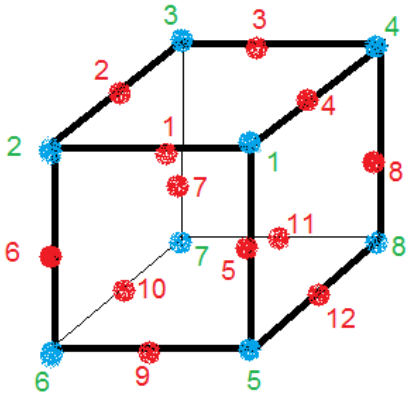
4) $(\mu\mu')\mu'' = \mu(\mu'\mu'')$

$(G^+, .)$ est bien un groupe.

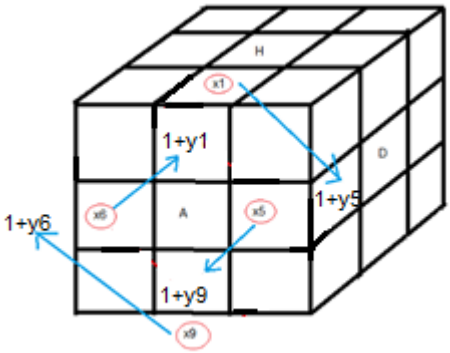
11.1 VÉRIFICATION

Les arêtes , sommets baladent partout, en baladant ils peuvent changer leur orientations, Il faut donc vérifier si la loi correspond bien avec le mouvement composé. Par ex AD .

Vérification pour les arêtes.



Numérotation des sommets et des arêtes



flèche bleue: $x'_1 = 1+x_5$

Suivons le mouvement des flèches bleues (flèche partant), le x_1 arrive (il bouge) à la facette $1+x_5$ et prend cette valeur c'est-à-dire $x'_1 = 1+x_5$
x_1 représente l'arête (bv) car il bouge

$x'_1 = 1+x_5$
$x'_5 = 1+x_9$
$x'_9 = 1+x_6$
$x'_6 = 1+x_1$

x' = a + p(x) avec p = (1,5,9,6) et a = (1,0,0,0,1,1,0,0,1,0,0,0)

Vérifions si ça correspond bien

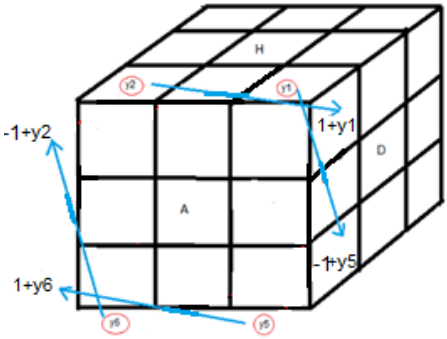
Pour D on a: D → (p',a') avec
p' = (4,8,12,5)
a' = 0

AD → (p,a)(p',a') = (pp', a + p(a'))
pp' = (1,5,9,6)(4,8,12,5) = (1,4,8,12,5,9,6)
p(a') = 0
a + p(a') = (1,0,0,0,1,1,0,0,1,0,0,0)

AD → (u,x) avec u = (1,4,8,12,5,9,6) et x = (1,0,0,0,1,1,0,0,1,0,0,0)
c'est exactement ce qui se passe pour les arêtes sur le Rubik's Cube !!!

Vérification pour les sommets:
A → (q,b)
D → (q',b')
AD → (q,b)(q',b') = ??
Il faut donc vérifier que '.' correspond bien avec le résultat des rotations AD

Observons la fig ci-dessous
Pour rotation A



flèche bleue: $y_1' = -1+y_5$

Suivons le mouvement des flèches bleues (flèche partant), le y_1 arrive (il bouge) à la facette $-1+y_5$ et prend cette valeur c'est-à-dire $y'_1 = -1+y_5$
y_1 représente le sommet (brv) car il bouge

$y'_1 = -1+y_5$
$y'_2 = 1+y_1$
$y'_5 = 1+y_6$
$y'_6 = -1+y_2$

$y' = b + q(y)$ avec $q = (1,5,6,2)$ et $b = (-1,1,0,0,1,-1,0,0)$

Pour D on a: $D \rightarrow (q',b')$ avec

$q' = (1,4,8,5)$
$b' = (1,0,0,-1,-1,0,0,1)$

AD → (q,b)(q',b') = (qq', b + q(b'))
qq' = (1,5,6,2)(1,4,8,5) = (2,4,8,5,6)
b = (-1,1,0,0,1,-1,0,0) , et q(b') = (-1,1,0,-1,0,0,0,1)
b + q(b') = (1,-1,0,-1,1,-1,0,1)

AD → (v,y) avec v = (2,4,8,5,6) et y = (1,-1,0,-1,1,-1,0,1)
c'est exactement ce qui se passe, pour les sommets sur le Rubik's Cube !!!

La loi '.' est bien:
(u,x,v,y)(u',x',v',y') = (uu',x+u(x'),vv',y+v(y'))

12 L'ENSEMBLE DES ÉTATS

On va définir une action libre et compatible '•' de M sur G^+ de façon suivante:

$G^+ \times M \to G^+$

$(\mu,V) \to \mu \bullet V = \nu \in G^+$

A_1) $\forall \mu$; $\mu \bullet I = \mu$;I fixe tout le monde

A_2) $\forall \mu,V,T$; $(\mu \bullet V) \bullet T = \mu \bullet (VT)$;associative

A_3) $a \in G^+$ donné, fixé

$\forall V \in M$, $a \bullet V = a \Rightarrow V = I$; librement

Quelqu'un qui laisse fixe un point est forcement I, I est la seule formule ayant des points fixes.

(12.1.1) A_4) $\forall \mu,V,T$; $\mu \bullet (VT) = (\mu \bullet V)(\mu \bullet T)$;compatibilité les lois de M et G^+

Remarques importantes :

i) L'axiome (A_3) montre que deux formules donnant le même état seront considérées comme identiques .

En effet :

$e \bullet V = e \bullet T$ il faut montrer V = T, allons-y

$(e \bullet V) \bullet T' = (e \bullet T) \bullet T'$

$e \bullet (VT') = e \bullet (TT')$

$e \bullet (VT') = e \bullet I = e$

d'après (A_3) $VT' = I \Longrightarrow V = T$

ii) L'axiome (A_3) implique que M est fini, en effet :

L'action '•' donne un morphisme de M sur S_{G^+}

$\zeta : M \rightarrow S_{G^+}$

$V \rightarrow \zeta(V) = p_v$; où p_v est une bijection de G^+

$p_v : G^+ \rightarrow G^+$

$\mu \rightarrow p_v(\mu) = \mu \bullet V$

ζ est un morphisme injectif en effet :

$\zeta(V) = id$

$p_v = id$

$p_v(\mu) = id(\mu) = \mu$

$\mu \bullet V = \mu \Rightarrow V = I$ (axiome A_3)

Or

$M/\mathrm{Ker}\ \zeta \simeq \mathrm{Im}\ \zeta \subset S_{G^+}$ fini

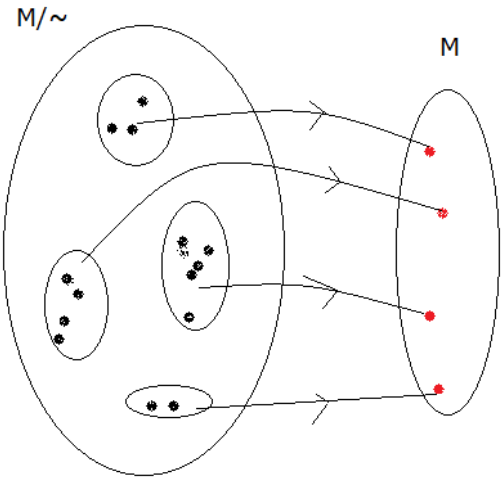
ζ injectif $\Rightarrow M \simeq \mathrm{Im}\ \zeta \subset S_{G^+} \Rightarrow M$ fini

Tout ceci revient à définir une relation d'équivalence $\sim$ sur M et identifier $M/\sim$ à M .

$V,T \in M$, $V \sim T \Leftrightarrow V, T \in \mathrm{Ker}\ \zeta$

$M/\sim = M/\mathrm{Ker}\ \zeta \simeq M \simeq \mathrm{Im}\ \zeta \subset S_{G^+}$ fini

comme G^+ est fini , $M/\sim$ est aussi fini et $|M/\sim| = |M|$



En pratique on considère ainsi:

Une formule est une suite finie de rotations de base {H,B,A,P,G,D} avec les règles suivantes :

* On convient d'éviter de faire HH', H'H, BB', B'B, AA', A'A etc ... dans une formule.

* Deux formules donnant le même état seront considérées comme identiques.

13 LE GROUPE DU RUBIK'S CUBE (G, .)

On pose

$G = \{\mu \in G^+ \mid \exists V \in M,\ e \bullet V = \mu\} \subset G^+$; e = l'état résolu.

Les éléments de G se nomment état, ce sont des configurations provenant de M (à partir de e) , c'est l'orbite de e.

Dans l'écriture 'e•V = μ' on dit que μ provient de V, ou V généré μ ou on atteint μ (à partir de e) par V, il y a une étonnante analogie avec la géométrie ...

Par ex pour l'écriture $\overrightarrow{AB} = \vec{u}$, on peut changer la notation, adoptons plutôt l'écriture $A \bullet \vec{u} = B$, on a le droit c'est simplement une notation, avec cette nouvelle écriture c'est beaucoup mieux, car on voit que $\vec{u}$ agit sur A pour donner B !! on dit que les vecteurs agissent sur les points, et

$A \bullet \vec{0} = A$; ($\overrightarrow{AA} = \vec{0}$)

on voit que $\overrightarrow{AA} = \vec{0}$ est un axiome, donc demander de démontrer que $\overrightarrow{AA} = \vec{0}$ n'a pas de sens !!!

de même

$(A \bullet \vec{u}) \bullet \vec{v} = A \bullet (\vec{u} + \vec{v}) \Rightarrow$

$A \bullet \vec{u} = B \ ; (\overrightarrow{AB} = \vec{u})$

$B \bullet \vec{v} = C \ ; (\overrightarrow{BC} = \vec{v})$

$A \bullet (\vec{u} + \vec{v}) = C$

$A \bullet (\overrightarrow{AB} + \overrightarrow{BC}) = C$

d'où

$\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$

Ce qui montre que la relation de Chasles est un axiome et que demander de démontrer que
$\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$

n'a pas de sens.

$\overrightarrow{AB} = \overrightarrow{CD}$ signifie que $\overrightarrow{AB}, \overrightarrow{CD}$ représentent un même vecteur, .

De même pour le Rubik's Cube

V = T signifie que V, T génèrent la même configuration.

Lorsqu'on fixe un point dans le plan par ex O, la relation:

$O \bullet \vec{u} = A$;espace affine '•' agit simplement transitif

montre une analogie en Rubik's Cube

$e \bullet V = \mu$;Rubik's Cube '•' agit librement

$O \Leftrightarrow e, \vec{u} \Leftrightarrow V$ et $A \Leftrightarrow \mu$

13.1 THÉORÈME FONDAMENTAL DE LA CUBOLOGIE

La question est suivante : Quelles sont les conditions nécessaires et suffisantes pour qu'une configuration soit un état , càd un élément de G^+ soit un élément de G ?

La réponse est connue sous le nom :

Théorème fondamentale de la Cubologie :

$\mu = (u,x,v,y) \in G^+$ est un élément de G ssi:

(F) $\sum x_i = 0 \pmod 2$ abrégé : $x = 0 \pmod 2$
(T) $\sum y_i = 0 \pmod 3$ abrégé : $y = 0 \pmod 3$
(P) sig(u) = sig(v)

Démonstration :

Conditions nécessaires

On se donne une formule $V \in M$, avec $e \bullet V = \mu = (u,x,v,y)$, il faut montrer que μ vérifie (F), (T) et (P).

¤ A) On constate que les rotations de base vérifient ces conditions :

(F) : Pour une rotation de base Z, e•Z=(p,a,q,b), d'après la table des orientations des arêtes (7.4.1) , on apporte soit 0, soit 4 le nombre d'orientations, donc a=0 (mod 2)

(T) : Pour une rotation de base Z, e•Z=(p,a,q,b), d'après la table des orientations des sommets (6.4.1) , on apporte soit 0, soit -1+1+1-1, 1-1-1+1, le nombre d'orientations, donc b=0 (mod 3)

(P) : Pour une rotation de base Z, e•Z=(p,a,q,b), on a: un 4-cycle-arêtes p, et un 4-cycle-sommets q,
donc sig(p) = sig (q).

¤ B) Raisonnons par récurrence

On va raisonner par récurrence sur la longueur de la formule |V| = n,

Ces propriétés sont vraies pour une rotation de base |Z|=1, càd pour n=1 ; d'après (A)

Supposons qu'elles sont vraies pour une formule Q de longueur n, |Q|=n , montrons qu'elles restent encore vraies pour une formule V de longueur [V|=n+1

Or on passe de longueur n à n+1 par une rotation de base Z

V = QZ ; |Q|=n

e•V = e•(QZ) = (e•Q)(e•Z) ; d'après l'axiome A4 (12.1.1)

(u',x',v',y') = (u,x,v,y) (p,a,q,b) = (up, x+u(a), vq, y+v(b)).

(F) : x' = x+u(a)

a = 0 (mod 2) ; d' après (A)

u(a) = 0 (mod 2) ; la permutation u ne change rien sur le modulo.

x = 0 (mod 2) ; HP

x' = x+u(a) = 0 (mod 2)

(T) : y' = y+v(b)

b = 0 (mod 3) ; d' après (A)

v(b) = 0 (mod 3) ; la permutation v ne change rien sur le modulo.

y = 0 (mod 3) ; HP
y' = y+v(b) = 0 (mod 3)

(P) : sig(u') = sig(up)

= sig(u) sig(p)

= sig(u) sig(q) ; d' après (A)

= sig(v) sig(q) ; HR

= sig(vq) = sig(v')

Conditions suffisantes

¤ On se donne un état μ de G càd une configuration qui vérifie (F), (T) et (P) , il faut trouver une formule V∈M telle que

e•V = μ.

La preuve est constructive, c'est-à-dire on construit petit à petit la formule V.
On va faire ça en plusieurs étapes.

On coupe (u, x, v, y) en deux morceaux

(u, x, v, y) = (u, x-u(x),v, y-v(y)) (id, x, id, y)

Ce coupage suggère l'algorithme de résolution suivant:

1) On place d'abord les arêtes comme exige u (ignorez les autres pièces)

2) On place les sommets comme exige v (sans déplacer les arêtes, ignorez l'orientation des arêtes, ignorez l'orientation des sommets)

3) On oriente les arêtes comme exige x (sans déplacer les arêtes, ni les sommets, ignorez l'orientation des sommets)

4) Et finalement on pivote les sommets comme exige y (sans toucher les arêtes sans déplacer les sommets)
On va faire ça en plusieurs étapes.

On prend 3 formules suivantes :

J = A[DH]A'H ⇒ permuter deux arêtes (HG)<->(HP).

Q = [DH]G'[HD]G ⇒ 3-cycle-sommets

(HGP)->(HAG)->(HPD) .

$J^2 = (A[DH]A'H)^2$ ⇒ pivoter deux arêtes $(HG)^-(HP)^-$.

$T = [DH]^2G'[HD]^2G$ ⇒ pivoter deux sommets $(HAG)^+(HGP)^-$.

Pour u : Placer les arêtes

Comme S_{12} est engendré par des transpositions on peut utiliser J (avec la conjugaison) pour placer les arêtes comme on veut, donc comme exige u .

Pour x-u(x) : On ignore cette étape car on orientera les arêtes plus tard.

Pour v : Placer les sommets

Quand on arrive ici, les arêtes sont bien placées (mais peut-être mal orientées) , la loi de parité (P) nous dit que v est pair car les arêtes sont bien placées , comme Q est un 3-cycle donc on peut utiliser Q (avec la conjugaison) pour placer les sommets (sans déplacer les arêtes) comme exige v (car les 3-cycles engendrent A_n) .

Pour y-v(y) : On ignore cette étape car on orientera les sommets plus tard.

Pour x : Orienter les arêtes

On utilise J^2 (avec la conjugaison) pour orienter les arêtes (sans déplacer les arêtes ni les sommets) comme exige x, c'est possible car la loi des flips (F) dit on oriente toujours 2 arêtes.

Pour y : Orienter les sommets

On utilise T (avec la conjugaison) pour orienter les sommets (sans déplacer les sommets , sans toucher les arêtes) comme exige y, c'est possible car la loi des twists (T) dit on pivote toujours 2 sommets de sens opposés ou 3 sommets dans le même sens.

Finalement on a trouvé une grosse grosse formule $N \in M$:

$\mu \bullet N = e$

donc il suffit de prendre $V = N' \in M$ et on aura :

$e \bullet V = \mu = (u, x\text{-}u(x), v, y\text{-}v(y))\ (id, x, id, y) = (u, x, v, y)$.

En fait la démonstration revient à résoudre le Cube par un algorithme qui utilise les trois formules J, Q, T.

Voyons maintenant si (G,.) est un groupe

On a montré que (théorème fondamental):

$G = \{\mu \in G^+ \mid (F), (T), (P) \text{ soient vérifiés}\} \subset G^+$.

G est donc l'ensemble des configurations vérifiant (F), (T), et (P).

Montrons que G est un sous groupe de G^+

1. $e = (id,0,id,0) \in G$ car e vérifie ces 3 lois

2. soient
$\mu = (u,x,v,y) \in G$ et
$\mu^{-1} = (u^{-1}, u^{-1}(-x), v^{-1}, v^{-1}(-y)) = (u',x',v',y')$ symétrique de μ

$x = 0 \pmod 2 \Rightarrow u^{-1}(-x) = 0 \pmod 2 \Longrightarrow x' = 0 \pmod 2$
de même pour $y' = 0 \pmod 3$

$sig(u') = sig(u^{-1})$
$sig(v') = sig(v^{-1})$
d'où
$sig(u') = sig(v')$
finalement $\mu^{-1} \in G$

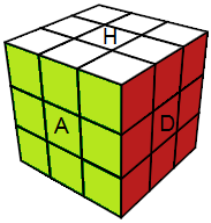
3. $\mu = (u,x,v,y)$, $\mu' = (u',x',v',y') \in G$
$\mu\mu' = (uu', x+u(x'), vv', y+v(y'))$
$x = 0 \pmod 2$
$x' = 0 \pmod 2$
$\Rightarrow x+u(x') = 0 \pmod 2$
$y = 0 \pmod 3$
$y' = 0 \pmod 3$
$\Rightarrow y+v(y') = 0 \pmod 3$

$sig(u) = sig(v)$
$sig(u') = sig(v')$
$sig(u)sig(u') = sig(v)sig(v')$
$\Rightarrow sig(uu') = sig(vv')$

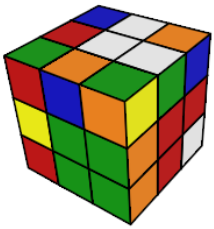
Ce qui prouve que $\mu\mu' \in G$,
G est bien un sous groupe de G^+
$G \subset G^+$, G est un sous groupe de G^+

Rappel : Par définition G est le groupe du Rubik's Cube.

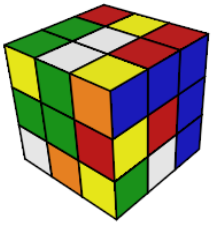
Voici la visualisation des états



état résolu



un état



un autre état

On peut voir que les centres ne sont pas bougés :
Haut=blanc, Avant=vert, Droite=rouge, ...
L'orientation du Cube reste intacte.

Un état est une configuration provenant de M en respectant l'orientation du Cube, càd on mélange le Cube avec les rotations de base sans bouger, ni tourner le Cube, c'est comme s'il y a un mécanisme qui fixe le Cube et on peut seulement tourner les faces.

On a:

$G = G^+ / \mathcal{N}$

où $\mathcal{N}$ sont les contraintes pour calculer $\mathcal{N}$ il suffit d'examiner les lois (F), (T), (P).

(F) : $x=0 \pmod 2 \rightarrow$ 2 choix

(T): $y=0 \pmod 3 \rightarrow$ 3 choix

(P): $sig(u)=sig(v) \rightarrow$ 2 choix

d'où

$\mathcal{N} = 2.3.2$

$G = G^+/\mathcal{N} = S_{12} \times \mathbb{Z}_2^{12} \times S_8 \times \mathbb{Z}_3^8/2.3.2$

$|G| = 12!.2^{12} \times 8!.3^8/2.3.2 = 12!.2^{10} \times 8!.3^7$

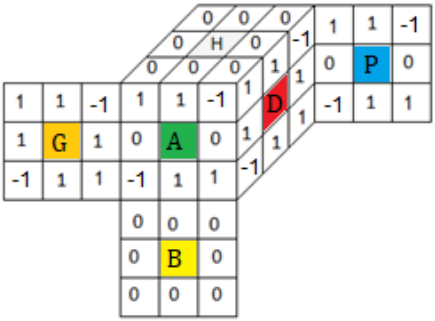
= 43 252 003 274 489 856 000

Remarque : on a aussi :

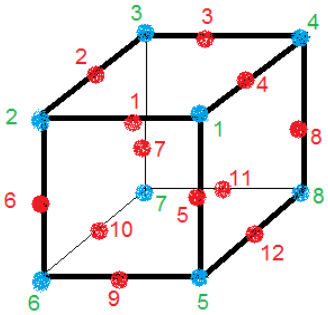
$G^+ = \{\mu = e \bullet V , V \in M^+\}$; e = l'état résolu.

l'ensemble des états provenant de M^+

13.2 L'ÉTAT ASSOCIÉ AUX ROTATIONS DE BASE



marquage



numérotation

Voici les états associés aux rotations de base H,B,A,P ...

e•H = μ_H = (p,a,q,b)
p = (1,2,3,4)
a = (0,0,0,0,0,0,0,0,0,0,0,0)
q = (1,2,3,4)
b = (0,0,0,0,0,0,0,0)

e•B = μ_B = (p,a,q,b)
p = (9,12,11,10)
a = (0,0,0,0,0,0,0,0,0,0,0,0)
q = (5,8,7,6)
b = (0,0,0,0,0,0,0,0)

e•A = μ_A = (p,a,q,b)
p = (1,5,9,6)
a = (1,0,0,0,1,1,0,0,1,0,0,0)
q = (1,5,6,2)
b = (-1,1,0,0,1,-1,0,0)

e•P = μ_P = (p,a,q,b)
p = (3,7,11,8)
a = (0,0,1,0,0,0,1,1,0,0,1,0)
q = (4,3,7,8)
b = (0,0,-1,1,0,0,1,-1)

e•G = μ_G = (p,a,q,b)
p = (2,6,10,7)
a = (0,0,0,0,0,0,0,0,0,0,0,0)
q = (3,2,6,7)
b = (0,-1,1,0,0,1,-1,0)

e•D = μ_D = (p,a,q,b)
p = (4,8,12,5)

a = (0,0,0,0,0,0,0,0,0,0,0,0)
q = (1,4,8,5)
b = (1,0,0,-1,-1,0,0,1)

NOTE:

1. Avec notre marquage:

* les rotations H,B,G,D ne modifient pas les orientations des arêtes seules les rotations A,P les modifient, elles apportent 4 flips,

* les rotations H,B, ne modifient pas les orientations des sommets seules les rotations A,P,G,D les modifient elles apportent 0 twists.

2. $e \bullet A = \mu_A = (p,a,q,b)$ et $e \bullet D = \mu_D = (p',a',q',b')$

On a bien

$e \bullet (AD) = \mu_{AD} = \mu_A \, \mu_D$

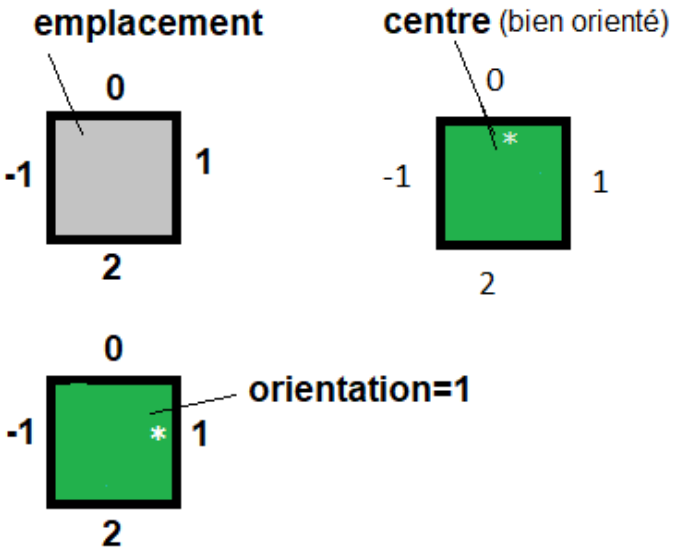
$= (p,a,q,b)(p',a',q',b') = (pp', a+p(a'), qq', b+q(b'))$

3. Parfois par abuse de langage on écrit A = (p,a,q,b) au lieu de e•A = (p,a,q,b).

13.3 ORIENTATION DES CENTRES

Si les centres sont orientés (avec une image par ex, comme le Rubik Hello Kitty, ou Rubik Pochmann ...) , le Rubik's Cube possède alors une 4ième loi, nommée loi des centres (C). en effet :

Un centre a 4 orientations et on oriente les centres ainsi :



* = 0, bien orienté

Come pour les arêtes, et les sommets
On décide arbitrairement un côté du centre est dominant,

et sur l'emplacement du centre on marque 0 (côté dominant), puis dans le sens horaire 1, 2, -1

Quand le côté dominant pointe sur 0, 1, 2, -1 on dit que l'orientations du centre vaut 0 (bien orienté) 1,2,-1.
Soit c la somme des orientations des 6 centres
$c = c_H + c_B + c_A + c_P + c_G + c_D$.

On voit que la loi des centres (C) est:
(C) : $(-1)^c = sig(u)$

Le nombre c d'orientation des centres est pair si sig(u) est paire, impair si sig(u) est impaire.

Si on pivote les centres sans toucher les autres pièces la signature des arêtes est paire (sig(arêtes) = 1) donc

$(-1)^c = 1$
$c = 2k$

càd le nombre d'orientations des centres est pair.

En passant par le degré
$90c = 180k$
90c = le nombre de degrés des centres ,

Donc quand on pivote les centres sans toucher les autres pièces le nombre de degrés des centres est un multiple de 180, autrement dit le nombre d'orientations (à 90°) des centres est paire.

Ceci explique pourquoi à l'état résolu, on a:
¤ Des centres à 180° .

¤ Ou des couples de centres à (90°,-90°)
¤ Ou des couples de centres à (90°,90°)
¤ Ou des couples de centres à (-90°,-90°)
etc ...

Dans une formule on compte les rotations de base +1, inverse -1
exp :

$A[DH]A'H \Longrightarrow 1+1+1-1-1-1+1 \Longrightarrow (H)^{+} = 90°$
$(DH)^{105} = I \Longrightarrow (D)^{+} = 90°$, $(H)^{+} = 90°$
$(DH')^{63} = I \Longrightarrow (D)^{-} = -90°$, $(H)^{+} = 90°$

On a $4^6/2 = 2048$ (divisé par 2 à cause de la loi $(1)^c = sig(u)$) configurations en plus. En effet le Super groupe est :

$G_s{}^{+} = S_{12} \times \mathbb{Z}_2{}^{12} \times S_8 \times \mathbb{Z}_3{}^8 \times \mathbb{Z}_4{}^6$

$\mu = (u, x, v, y, c)$ $u \in S_{12}$, $x \in \mathbb{Z}_2{}^{12}$, $v \in S_8$, $y \in \mathbb{Z}_3{}^8$, $c \in \mathbb{Z}_4{}^6$

On définit la loi dans $G_s{}^{+}$ comme suite:

$\mu, \mu' \in G_s{}^{+}$

$\mu = (u,x,v,y,c)$ et $\mu' = (u',x',v',y',c')$
$\mu\mu' = (u,x,v,y,c)(u',x',v',y',c') =$

$= (uu', x+u(x'), vv', y+v(y'), c+c')$

où

$uu' = u'ou$,

$u(x) = (x_{u(1)}, x_{u(2)}, x_{u(3)},..., x_{u(12)})$; permutation des x_i par u

$|G_s| = 12! .2^{12} \times 8!.3^8 \times 4^6/2.3.2.2$

$= 12! . 2^{10} .8!.3^7 . 2^{11} = 88\ 580\ 102\ 706\ 155\ 225\ 088\ 000$

$|G_s| = 2048|G|$

Remarque :

la formule :

$|G_e^+| = |G| = |M| / |M_e|$

$G_e^+ = \{ \mu \in G^+ \mid \mu = e \bullet V , V \in M\} = G$ = l'orbite de e

$M_e = \{ V \in M \mid e \bullet V = e\}$ = stabilisateur de e.

Comme aucune formule laisse fixe un état sauf I on a:

$M_e = \{I\}$

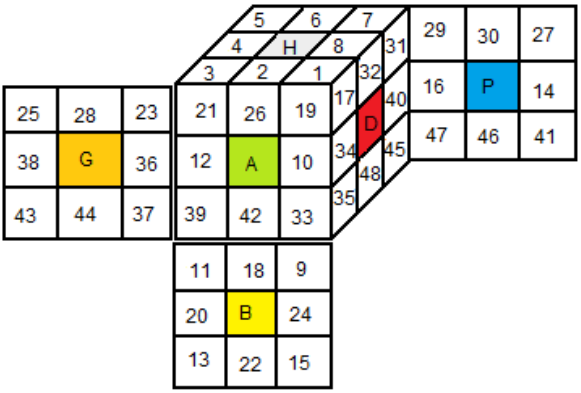
d'où $|G| = |M|$.

14 PERMUTATIONS DES AUTOCOLLANTS (Λ, .)

Soit X = {1,2,3, ..., 48} l'ensemble des autocollants (stickers) du Rubik's Cube. On numérote les autocollants de la façon suivant. Une fois numérotés on peut regrouper facilement ces autocollants pour former les arêtes, et les sommets .

* Pour les arêtes : autocollants pairs
On commence par les facettes dominantes: 2, 4, 6, 8, ...
puis les autres facettes de l'arête : (2,26), (4,28), (6,30) , ...
x_i = (2i, 2i+24)

* Pour les sommets : autocollants impairs
On commence par les facettes dominantes: 1,3,4,7, ...
puis les autres facettes dans le sens horaire : (1,17,19), (3,21,23), (5,25,27) , ...
y_i = (2i-1,4i+13,4i+15)
Et voici la numérotation des autocollants

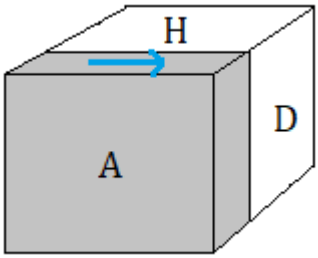


Numérotation des autocollants X

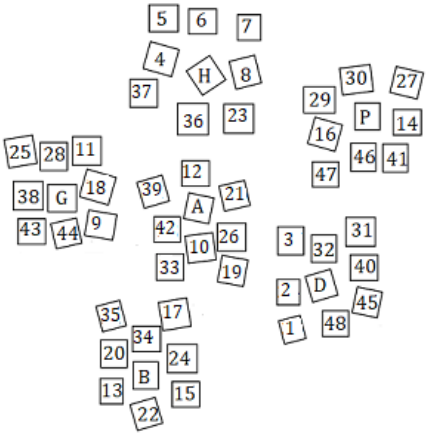
les autocollants éparpillés sur la table

14.1 ACTION DU GROUPE M SUR X

D'un côté on a un Rubik's Cube monochrome, de l'autre côté on a les autocollants numérotés, éparpillées sur la table, physiquement rien ne lie entre le Rubik's Cube monochrome et les autocollants . Imaginez lorsqu'on fait une rotation A par ex, une force mystérieuse déplace ces autocollants ....



Rotation A



autocollants déplacées

On appelle ceci "action" de A sur X, en générale on note l'action par '•'
Au lieu de prendre la rotation A, on peut prendre n'importe quel élément de M, on dit que M agit sur X.
On définit alors une action libre '•' de M sur X vérifiant les propriétés suivantes :
$X \times M \dashrightarrow X$
$(x,V) \dashrightarrow x \bullet V = x' \in X$

$B_1)$ $\forall x , x \bullet I = x$
$B_2)$ $\forall x, V,T ; (x \bullet V) \bullet T = x \bullet (VT)$
$B_3)$ $a \in X$ donné, fixé
$\forall V \in M,\ a \bullet V = a \Rightarrow V = I$; librement
Quelqu'un qui laisse fixe un point est forcement I, I est la seule formule ayant des points fixes.

Se donner l'action '•' revient à se donner un morphisme ζ de $(M, .)$ sur $(S_{48}, .)$ $(S_{48} = S_X)$ vérifiant :

$\zeta : M \to S_{48}$
$V \to \zeta(V) = p_V \in S_{48}$; $p_V(x) = x \bullet V$, permutation de X

$C_1)$ $p_I = id$
$C_2)$ $p_{VT} = p_V \, p_T$
$C_3)$ $p_V = p_T \Rightarrow V = T$

L'axiome (C_3) montre que deux formules donnant la même permutation seront considérées comme identiques.

l'axiome (C_3) signifie que ζ est injectif on a donc

$M/\mathrm{Ker}\,\zeta \simeq M \simeq \mathrm{Im}\,\zeta \subset S_{48} \Rightarrow M$ fini

À chaque formule V∈M on associe une permutation p_V de S_{48} en particulier à chaque rotation de base {H,B,A,P,G,D} on associe une permutation (des autocollants) {p_H, p_B, p_A, p_P, p_G, p_D} de S_{48} et soit Λ l'ensemble des permutations engendrées par : {p_H, p_B, p_A, p_P, p_G, p_D}

$\Lambda = < p_H, p_B, p_A, p_P, p_G, p_D >$ et
$\Lambda^+ = < p_H, p_B, p_A, p_P, p_G, p_D, p_\Gamma, p_\psi, p_\Omega >$

La construction de Λ a besoin de X c'est pourquoi dans la définition d'un twist, les autocollants jouent un rôle primordial .

Rappel : on définit sur Λ une loi de composition '.'

ρ, σ ∈Λ

ρ . σ = σ o ρ

(Λ, .) est un groupe , on écrit ρσ = ρ.σ on a donc deux groupe (M, .) et (Λ, .) le groupe des formules et le groupe des permutations (des autocollants) du Rubik's Cube.

On a :

$|\Lambda^+| = |G^+|$

$|\Lambda| = |G|$

<u>Permutations standards</u>
2-cycle-arêtes, 3-cycle-sommets :

pH := (2,4,6,8)(26,28,30,32)
(1,3,5,7)(17,21,25,29)(19,23,27,31) ;

```
pB := (18,24,22,20)(42,48,46,44)
(9,15,13,11)(33,45,41,37)(35,47,43,39);
pA := (2,34,18,36)(26,10,42,12)
(1,35,11,23)(17,9,37,3)(19,33,39,21);
pP := (6,38,22,40)(30,14,46,16)
(7,25,13,45)(29,27,41,47)(31,5,43 ,15);
pG := (4,12,20,14)(28,36,44,38)
(3,39,13,27)(21,11,41,5)(23,37,43,25);
pD := (8,16,24,10)(32,40,48,34)
(1,29,15,33)(17,31,45,35)(19,7,47,9);
```

Permutations étendues

```
pGamma := (2,26);
pPsi := (1,17,19);
pOmega := (2,8)(26,32);
```

Permutations tranches

```
ph := (10,36,14,40)(34,12,38,16);
pd := (2,30,22,42)(26,6,46,18);
pa :=  (4,32,24,44)(28,8,48,20);

Lambdaplus :=  Group( pH, pB, pA, pP, pG, pD, pGamma,
pPsi, pOmega );
Lambda1 := Group( pH, pB, pA, pP, pG, pD );

Print( "\n" );
Print( "|Lambda+| = ",Size( Lambdaplus ), "\n" );
Print( "|Lambda| = ", Size( Lambda1 ) , "\n" );
Print( "N = ", 2 * 3 * 2 , "\n" );
Print( "|G+| = ", Factorial(12) * 2^12 * Factorial(8) * 3^8 ,
"\n" );
```

Print("|G| = |G+|/N = ", Factorial(12) * 2^12 * Factorial(8) * 3^8 / (2 * 3 * 2), "\n");

Le GAP
Télécharger le GAP ici :
https://www.gap-system.org/Releases/4.4.12.html

Dans la fenêtre de cmd on se place dans le dossier de GAP
C:\Users\nom> cd\gap4r4\bin
C:\gap4r4\bin>gap < gap_rubikcube.txt

```
gap> (1,3,5,7)(2,4,6,8)(17,21,25,29)(19,23,27,31)(26,28,30,32)
gap> (9,15,13,11)(18,24,22,20)(33,45,41,37)(35,47,43,39)(42,48,46,44)
gap> (1,35,11,23)(2,34,18,36)(3,17,9,37)(10,42,12,26)(19,33,39,21)
gap> (5,43,15,31)(6,38,22,40)(7,25,13,45)(14,46,16,30)(27,41,47,29)
gap> (3,39,13,27)(4,12,20,14)(5,21,11,41)(23,37,43,25)(28,36,44,38)
gap> (1,29,15,33)(7,47,9,19)(8,16,24,10)(17,31,45,35)(32,40,48,34)
gap> (2,26)
gap> (1,17,19)
gap> (2,8)(26,32)
gap> (10,36,14,40)(12,38,16,34)
gap> (2,30,22,42)(6,46,18,26)
gap> (4,32,24,44)(8,48,20,28)
gap> <permutation group with 9 generators>
gap> <permutation group with 6 generators>
gap> gap>
gap> |Lambda+| = 519024039293878272000
gap> |Lambda| = 43252003274489856000
gap> N = 12
gap> |G+| = 519024039293878272000
gap> |G| = |G+|/N = 43252003274489856000
gap> gap>
C:\GAP4R4\bin>
```

Remarque important

Une remarque importante sur M, dans M on peut avoir

I , AAAA, AAAAAAAA, AAAAAAAAAAAA , ...
D', DDD, DDDDDD, DDDDDDDDD, ...
etc ...

Ce qui montre que M a une infinité d'éléments, or on sait que le groupe du Rubik's Cube est fini, on aimerait donc que M lui aussi soit fini, et avoir le même nombre d'éléments que le groupe du Rubik's Cube. C'est pourquoi on a ajouté l' axiome (C_3) qui signifie que deux formules seront identiques si elles donnent la même permutation.

$p_I = p_{AAAA} = p_{AAAAAAAA} \Rightarrow I = AAAA = AAAAAAAA$

$p_{D'} = p_{DDD} \Rightarrow D' = D^3$

Autrement dit on met toutes les formules T ayant p_v comme permutation dans la boîte V (T=V) et comme S_{48} est fini, donc M est aussi fini.

De façon plus précise on passe par ce qu'on appelle le groupe libre ....

<u>Groupe libre</u>

On se donne 2 ensembles finis :

X={a,b,c,d,...} et X' = {a',b',c',d',...} disjoints et en bijection a→a', b→b' ... et un élément 1 non dans X ni dans X'. On forme alors les mots de X c'est-à-dire les suites finies d'éléments de X ou X' avec la règle: aa', a'a, bb', b'b, cc', c'c, ... interdits dans un mot.
du genre

V = abd'bbc ; OK
T = c'dab'bd^2 ; interdit (à cause b'b)
On pose :
aa' = a'a = bb' = b'b = cc' = c'c = ... = 1

Soit F_x = < a, b, c, d, ... > l'ensemble des mots de X , muni la loi concaténation, on a:
1. Loi interne (évident)
2. 1 = élément neutre (par déf)
3. a' ⇒ symétrique de a (par déf)
   aa' = a'a = 1 et
   V = adb'c ⇒ V' = c'bd'a' symétrique de V
4. (VT)S = V(TS) (à démontrer)

F_x forme alors un groupe nommé groupe libre engendré par X . On peut remarquer que F_x est infini, en effet on peut former un mot de longueur comme en veut !

Le problème du groupe libre est le suivant: Comment rendre F_x fini ? l'idée c'est trouver un morphisme injectif sur un groupe fini L .

On se donne un groupe L fini et un morphisme f injectif, à chaque mot V de F_x on associe un élément de L

f: $F_x \to L$; f injectif
1. f(1) = e ; e=élément neutre de L
2. V,T ∈F_x , f(VT) = f(V)f(T)

$F_x/Ker(f) \simeq Im(f)$ (c'est un théorème)
comme f est injectif ⇒ $F_x/Ker(f) \simeq F_x \simeq Im(f) \subset$ L fini ⇒ F_x fini

Pour nous
X = {H,B,A,P,G,D} , F_x = M
L = Λ = < p_H, p_B, p_A, p_P, p_G, p_D > ⊂ S_{48} fini

ρ: M → Λ ; ρ surjection
H → ρ(H)=p_H, B → ρ(B)=p_B, A → ρ(A)=p_A, ... ∈ S_{48}

1. $I \rightarrow \rho(I) = p_I = id$
2. $VT \rightarrow \rho(VT) = p_{VT} = p_V\, p_T$

$V,T \in M$, $V \sim T \Leftrightarrow p_V = p_T$
Et la loi quotient : $\underline{V}\ \underline{T} = \underline{VT}$ dans $M/\sim$
Φ: $M/\sim \dashrightarrow \Lambda$
$\underline{V} \rightarrow \Phi(\underline{V}) = p_V$

comme ρ est une surjection on a $M/\sim \simeq \Lambda$ donc $|M/\sim| = |\Lambda|$.

il est plus simple de manipuler
$M = < H, B, A, P, G, D >$; avec la <u>convention</u> $V = T$ si V et T donnent la même permutation $p_V = p_T$
que de manipuler les classes d'équivalences $M/\sim$

Comme on considère que deux formules donnant la même permutation sont identiques , on dira alors qu'une formule possède des différentes écritures (de représentants) comme par ex:

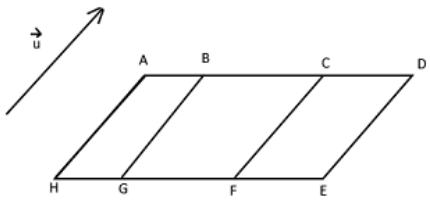
$I = A^4 = A^8 = [HD]^6$
$D' = D^3$
$HB = BH$
$(H^2D^2)^3(B^2D^2)^3 = (H^2G^2)^3(B^2G^2)^3$
$(A^2P'D'H'B)^2 = (HDA^2PB')^2$
.....

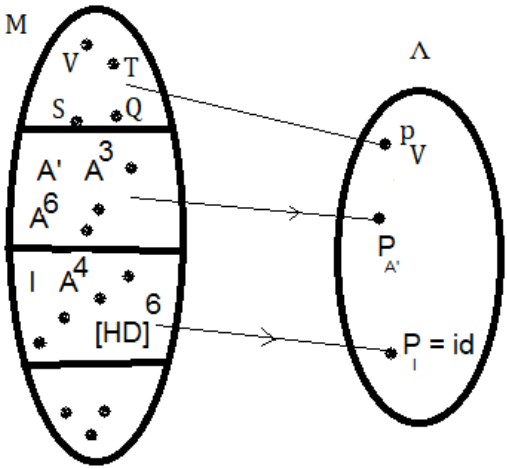
* Comme pour les nombres, l'inverse de 2 a plusieurs l'écriture : 1/2 = 3/6 = 0,5 ... mais on a un seul l'inverse de 2

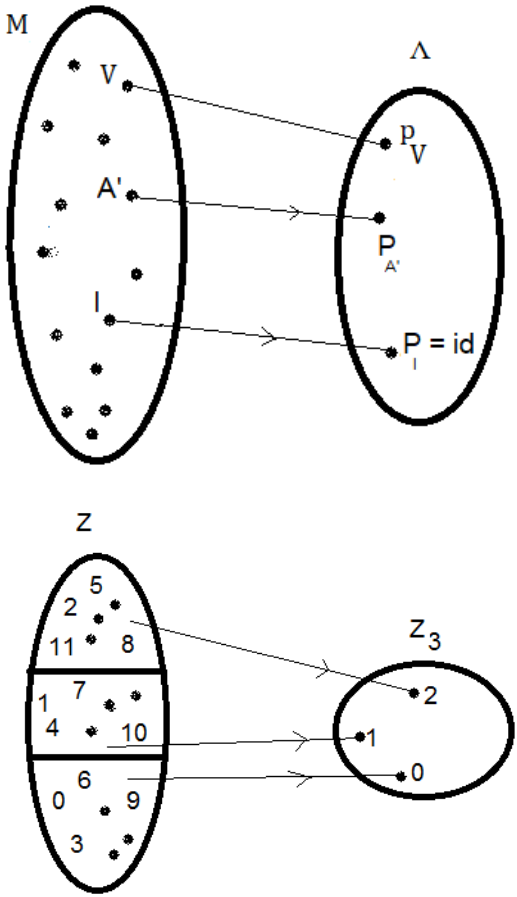
* On a un seul vecteur $\vec{u}$ mais on a plusieurs écritures

$\vec{u} = \overrightarrow{HA} = \overrightarrow{GB} = \overrightarrow{FC} = \overrightarrow{ED} = \ldots$

$\vec{0} = \overrightarrow{AA} = \overrightarrow{BB} = \ldots$





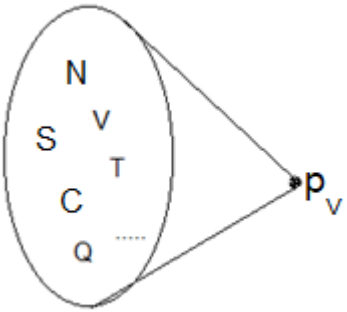


Logiquement une formule c'est une classe d'équivalence d'écritures, mais comme on ne manipule les formules que par ses représentants , c'est pourquoi par abuse de langage on appelle l'écriture : 'formule'.
Résumons : il y a une seule formule V donnant la permutation p_V , mais il y a plusieurs d'écritures de V. En

pratique, on oublie les classes d'équivalence, on considère simplement:

* formule (resp. étendue) ⇒ une suite finie de rotations (resp. contenant au moins une rotation étendue) de base .

* deux formules identiques si elles donnent la même permutation .



Parmi les formules N, S, V, T, C, Q , ... qui donnent la permutation p_V , il y a des plus courtes , des plus structurées etc ... en général on utilise des plus courtes .

Dans l'écriture 'p_V' on dit que p_V provient de V, ou généré par V .

<u>En résumé</u> :
Chaque <u>formule</u> génère une <u>permutations</u> (des autocollants) .

Il est donc important de faire la distinction entre: formule, et permutation . Λ c'est l'ensemble des permutations

produits par M , il y a donc une distinction entre A (rotation) et p_A (permutation).

* L'axiome (A_4) relie les lois de (M, .) de (G, .) et de (Λ, .)
$VT \Leftrightarrow (e \bullet V)(e \bullet T) \Leftrightarrow p_V\, p_T$
c'est-à-dire :

¤ $V \to \mu$, $T \to \nu \Rightarrow VT \to \mu\nu$
¤ $V \to p_V$, $T \to p_T \Rightarrow VT \to p_V\, p_T$
¤ $e \bullet V \to p_V$, $e \bullet T \to p_T \Rightarrow (e \bullet V)(e \bullet T) \to p_V\, p_T$

* Attention !! il y a plusieurs actions '•' :

¤ l'actions '$\bullet_1$' de M sur G^+ l'ensemble des configurations.
'$\bullet_1$' : $G^+ \times M \to G^+$

¤ et l'action '$\bullet_2$' de M sur X={1, 2, 3, ..., 48} l'ensemble des autocollants.
'$\bullet_2$' : $X \times M \to X$

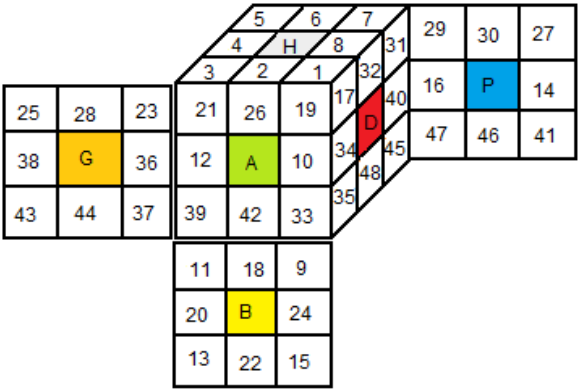
15 CONNEXION ENTRE Λ ET G

On rappelle que

$x_i = (2i, 2i+24)$

$y_i = (2i-1,4i+13,4i+15)$

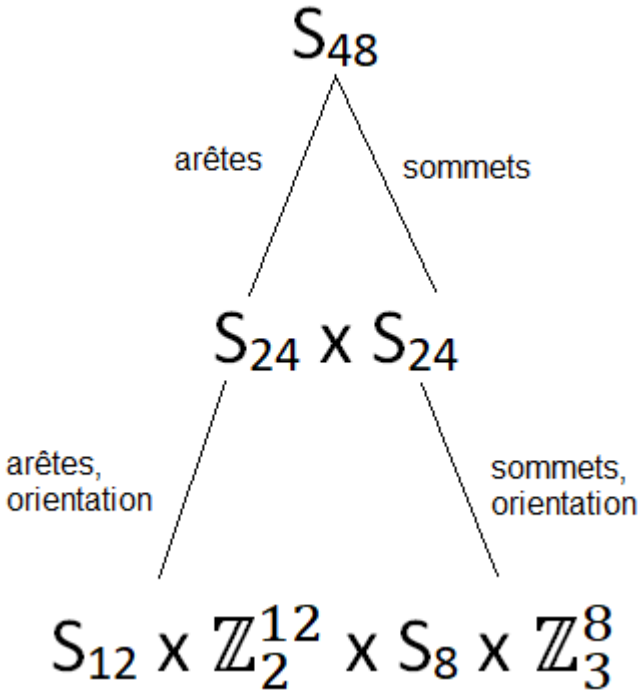
$\Lambda = < p_H, p_B, p_A, p_P, p_G, p_D >$



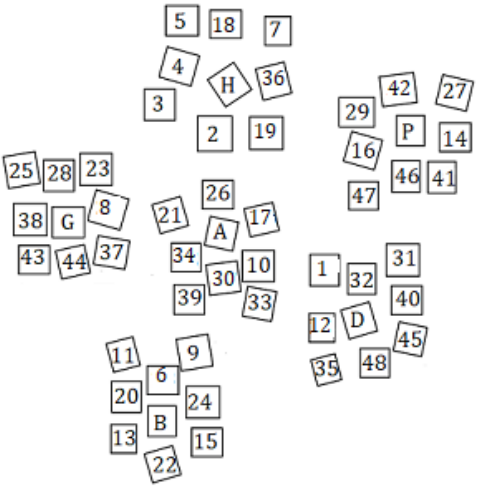
Numérotation des autocollants

Les permutations de Λ : $p_H, p_B, \ldots \in S_{48}$ ne sont pas quelconque de X={1,2,3,...,48} mais elles sont très particulières pour voir cela il suffit de suivre le mouvement des autocollants, l'autocollant '1' par exemple,

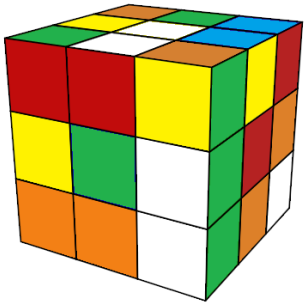
il ne peut pas se placer en '34' par ex , ou encore à chaque fois que '1' bouge , l'autocollant '17' bouge aussi... le '1' a un mouvement de S_8 et de rotation autour d'un triangle équilatérale (le '1' peut se placer en '17' ou '19'). les p_H, p_B, ... sont alors décomposées en 4 morceaux ainsi :



Ce ci nous suggère une relation entre Λ er G.



(a) → p_V



(b) → μ=e•V

L' images (a) représente une permutation p_V et l'image (b) représente un état μ provient de V (μ=e•V).

On se donne donc p_V et on veut trouver l'état $\mu=(u,x,v,y)$ correspondant. Pour fixer les idées on prend par ex p_A:

$p_A = (2,34,18,36)(26,10,42,12)$
$(1,35,11,23)(9,37,3,17)(19,33,39,21)$

<u>Les arêtes</u>

or $x_i = (2i, 2i+24)$ d'où

$(2,26) = x_1$

$(10,34) = x_5$

$(18,42) = x_9$

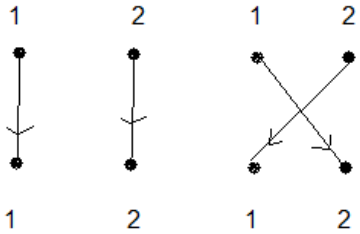
$(12,36) = x_6$

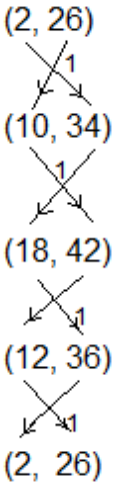
de

$\sigma = (2,34,18,36)(26,10,42,12)$

on en déduit

$* (2,34,18,36) \Rightarrow x_1 \to x_5 \to x_9 \to x_6 \Rightarrow u = (1,5,9,6)$





$2 \dashrightarrow 34 \Rightarrow x_1 \dashrightarrow 1+x_5 \Rightarrow$ l'orientation de $x_1 = 1$

$10 \dashrightarrow 42 \Rightarrow x_5 \dashrightarrow 1+x_9 \Rightarrow$ l'orientation de $x_5 = 1$

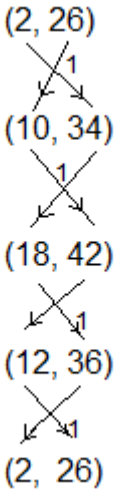
$18 \dashrightarrow 36 \Rightarrow x_9 \dashrightarrow 1+x_6 \Rightarrow$ l'orientation de $x_9 = 1$

$12 \dashrightarrow 26 \Rightarrow x_6 \dashrightarrow 1+x_1 \Rightarrow$ l'orientation de $x_6 = 1$

$x = (1,0,0,0,1,1,0,0,1,0,0,0)$

inversement de $u = (1,5,9,6)$ et $x = (1,0,0,0,1,1,0,0,1,0,0,0)$
on doit retrouver σ

$u = (1,5,9,6) \Rightarrow x_1 \rightarrow x_5 \rightarrow x_9 \rightarrow x_6$



en suivant les flèches , ça donne :

$\sigma = (2,34,18,36)(26,10,42,12)$

<u>Les sommets</u>

* De même pour les sommets , on a :

$y_i = (2i-1,4i+13,4i+15)$ d' où

$(1,17,19) = y_1$

$(9,33,35) = y_5$

$(11,37,39) = y_6$

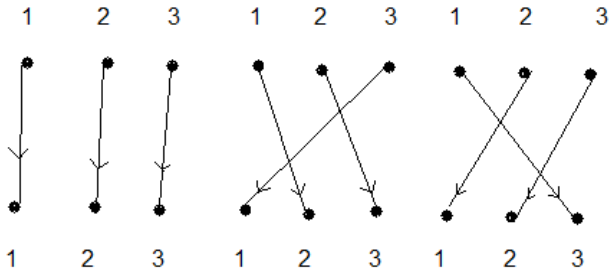
$(3,21,23) = y_2$

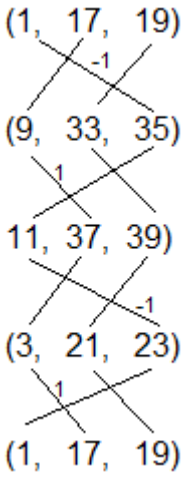
de

$\rho = (1,35,11,23)(9,37,3,17)(19,33,39,21)$;

on en déduit

* $(1,35,11,23) \Rightarrow y_1 \to y_5 \to y_6 \to y_2 \Rightarrow v = (1,5,6,2)$





$1 \to 35 \Rightarrow y_1 \to -1+y_5 \Rightarrow$ l'orientation de $y_1 = -1$

$9 \to 37 \Rightarrow y_5 \to 1+y_6 \Rightarrow$ l'orientation de $y_5 = 1$

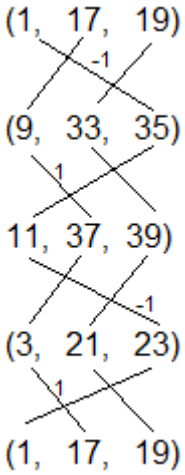
$11 \to 23 \Rightarrow y_6 \to -1+y_2 \Rightarrow$ l'orientation de $y_6 = -1$

$3 \to 17 \Rightarrow y_2 \to 1+y_1 \Rightarrow$ l'orientation de $y_2 = 1$

y = (-1,1,0,0,1,-1,0,0)

inversement de v = (1,5,6,2) et y = (-1,1,0,0,1,-1,0,0) on doit retrouver ρ

* $v = (1,5,6,2) \Rightarrow y_1 \to y_5 \to y_6 \to y_2$



en suivant les flèches , ça donne :

ρ = (1,35,11,23)(9,37,3,17)(19,33,39,21)

finalement on retrouve bien μ_A .

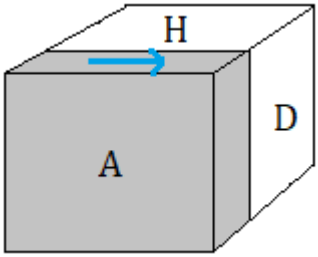
$p_A \Leftrightarrow \mu_A = (u,x,v,y)$

On trouve ainsi G^+ :

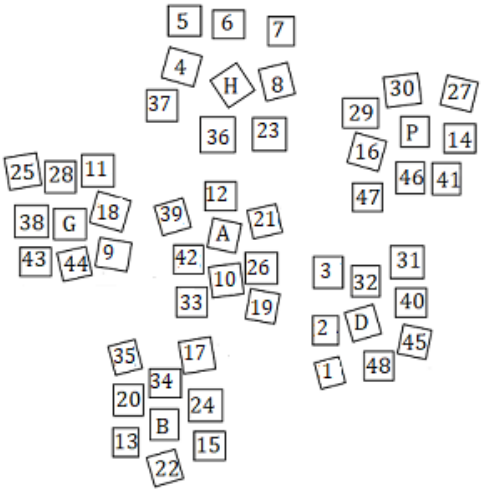
$G^+ = (S_{12} \times Z_2^{12}) \times (S_8 \times Z_3^8)$

<u>En résumé</u> :

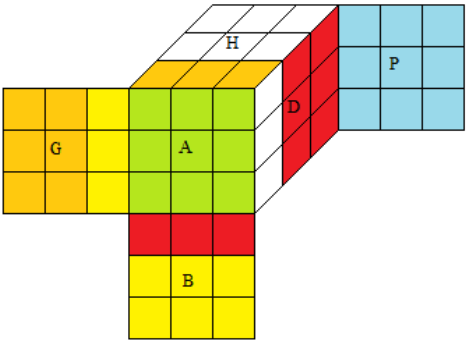
$A \Rightarrow p_A \Rightarrow \mu_A$



Rotation A



permutation p_A



état μ_A

Il est donc important de faire la distinction entre: formule, permutation, état.

J'insiste sur la différence entre ses objets: A, p_A, μ_A

A = rotation (formule, mouvement)
p_A = permutation (des autocollants)
μ_A = état (configuration, motif)

16 TROIS ANTAGONISMES M,Λ,G

L'étude mathématique du Rubik's Cube fait intervenir 3 antagonismes M, Λ, G .

M = <H, B, A, P, G, D>, formules
Λ = <p_H, p_B, p_A, p_P, p_G, p_D> (Λ ⊂ S_x), permutations (des autocollants)
G = les états

On peut se poser la question si ces ensembles sont équipotents (↔) ?
la réponse est affirmative.

ρ: M -→ Λ
A -→ ρ(A) = p_A
ρ(I) = id, ρ(H) = p_H ... etc
ρ est clairement un morphisme, en effet quand on fait les rotations AB on permute d'abord p_A puis p_B
ρ(AB) = $p_A p_B$ = ρ(A)ρ(B)

¤ ρ est injective (axiome A_3) en effet $p_V = p_T \Rightarrow V = T$ deux formules donnant la même permutation sont identiques.

¤ ρ est surjective par ex
$p = p_A^2 p_B p_H^{-1}$
soit
V = A^2BH' on a

$\rho(V) = \rho(A^2BH') = \rho(A^2)\rho(B)\rho(H') = \rho^2(A)\rho(B)\rho^{-1}(H)$
$= p_A^2 p_B p_H^{-1} = p$
donc M et Λ sont en bijection : M ↔ Λ

Pour M et G c'est la même chose
σ: M -→ G
V -→ σ(V) = e•V = μ

¤ σ est injective (Axiome A_3) en effet e•V = e•T ⇒ V = T
deux formule donnant le même état sont identiques.

¤ σ est surjective , la définition de G montre σ est surjective

Soit μ un état , il provient donc une formule V

e•V = μ

ça signifie σ(V) = μ

donc M et G sont en bijection : M ↔ G

Note:

1. M, Λ, G jouent des rôles différents.

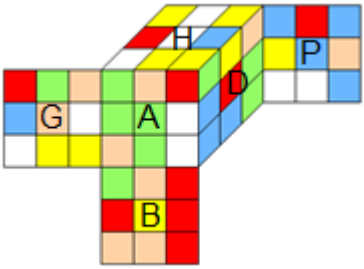
2. |M| = |Λ| = |G|

L'un des plus grand difficulté lorsqu'on étudie mathématiquement le Rubik's Cube c'est définir son groupe G.

Il y a là beaucoup de confusion, on lit souvent c'est Λ, puis parfois c'est M et parfois même c'est Im(f) où f: M→S_{48} .

Tout ceci provient de la confusion entre une rotation, une permutation et un état !! .

Mélangez votre Rubik's Cube, et posez le sur une table en respectant Haut=blanc, Avant=vert, Droite=rouge, ... puis prenez les photos de ses 6 faces elles forment ainsi un motif nous dirons un état, ce sont ces états qui décrivent vraiment le Rubik's Cube.



Voici un état

Le problème est : Comment "coder" ces états mathématiquement ? et comment définir une loi de composition sur ces états ?

¤ M ne "visualise" pas le Cube puisque ce sont des suites finies de rotations $AHBPD'H^2$ ... on ne voit ni arêtes, ni sommets , ni orientation des pièces or si vous tenez le Rubik's Cube en main vous voyez bien qu'il a des arêtes, des sommets, et ces pièces sont orientées !

¤ Λ lui non plus ne "visualise" pas le Cube pour les même raisons. Λ sont des permutations "brute" des autocollants qui sont éparpillés sur la table là non plus on ne voit ni

arêtes ni sommets, ni orientation , il n'y a que des numéros qui bougent !

Donc ni les rotations, ni les permutations (des autocollants) décrivent le Cube, seuls les états (les motifs) décrivent le Cube en effet dans $\mu = (u,x,v,y)$ on voit bien les arêtes 'u', l'orientation des arêtes 'x', les sommets 'v' et l'orientation des sommets 'y' . Ces trois groupes M, Λ, G jouent des rôles différents , M agit sur X mais ni Λ ni G agit sur X. On voit bien quand on tourne une face les autocollants se déplacent, mais pas le contraire !

La définition du groupe G du Rubik's Cube est :

$G = \{\mu \in G^+ / \exists V \in M , e \bullet V = \mu\}$

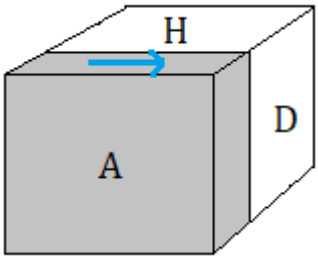
Il faut maintenant définir ce que c'est :

(i) $(G^+, .)$ groupe : $G^+ = ?$, $'.' = ?$,

(ii) $(M, .)$ groupe : $M = ?$, $'.' = ?$,

(iii) $'\bullet' = ?$, $e = ?$

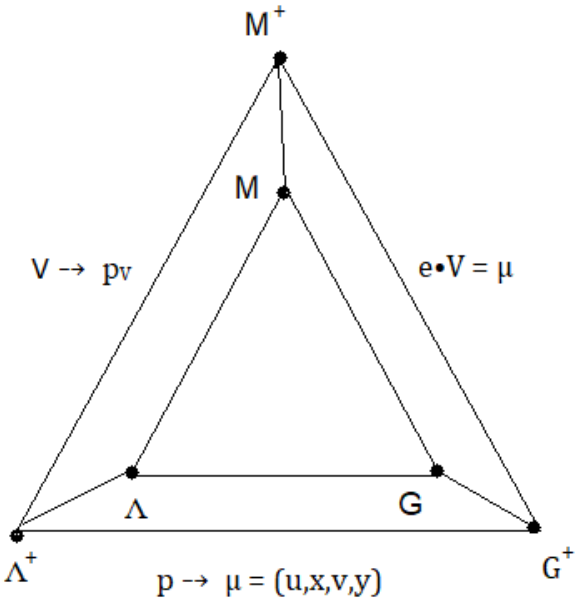
Pour arriver il fallait utiliser tout un technique ... le marquage, la couleur dominante, le numérotation des pièces , l'orientation , l' action un groupe etc ...



M: Les formules (rotations)

Λ : Les permutations (des stickers)

G: Les états (motif)



→On utilise M pour fabriquer les algorithmes de résolutions.

→On utilise Λ pour calculer le cardinal de G.

→On utilise G pour d'écrire le Rubik's Cube : Les lois, les propriétés ...

NOTE :

Dans l'écriture "a = b" certaine c'est de vraie l'égalité, certaine c'est une simple abréviation par ex:

$\varphi = APH^2DA^2.D^2P^2H'BA.H^2D'G'HP^2.BD^2HP^2H$

c'est une abréviation, car à gauche de '=' c'est un état, et à droite de '=' c'est une formule donc ça ne peut pas être égal ! ça signifie simplement: pour obtenir l'état φ on applique la formule, où la formule donne l'état φ

(HP)→(HD)→(AD) = [HD] (abréviation)

de même à gauche c'est une permutation et à droite c'est une formule donc ça ne peut pas être égal ! ça signifie simplement pour déplacer ces arêtes on applique la formule [HD], ou [HD] déplace ces arêtes ainsi.

e•V = μ ;(égalité)

$A' = A^3$;(égalité car $A^4 = I$ l'ordre 4)

$(H^2D^2)^3(B^2D^2)^3 = (H^2G^2)^3(B^2G^2)^3$;(égalité, comme $\frac{1}{2} = \frac{3}{6}$)

$B = (DG'A^2P^2DG')\ H\ (DG'A^2P^2DG')$;(égalité)

A = (p,a,q,b) ;(abréviation)

A = (2,34,18,36)(26,10,42,12)
(1,35,11,23)(9,37,3,17)(19,33,39,21) ; (abréviation)

α = (p,a,q,b) ; (égalité)

17 LE NOMBRE D'ÉTATS

La première idée est se demander combien y-a-t-il d'éléments dans G ?, c-à-d combien y-a-t-il d'états ?
Avec les 3 loi qu'on vient de découvrir, on peut alors répondre à cette question:

1. La loi des flips dit que $\sum x_i = 0 \pmod 2$ donc si 11 arêtes sont bien orientées alors la 12ème aussi, sinon on aura $\sum x_i = 1 \pmod 2$ donc on n'a besoin que Z_2^{11} au lieu de Z_2^{12}

2. Même choses pour les sommets, la loi des twists dit $\sum y_i = 0 \pmod 3$ donc si 7 sommets sont bien orientés alors le 8ème aussi, sinon on aura $\sum y_i = 1$ ou $2 \pmod 3$ donc on n'a besoin que Z_3^7 au lieu de Z_3^8

finalement G est contenu dans
$G \subset S_{12} \times Z_2^{11} \times S_8 \times Z_3^7$

3. La loi de parité dit $\mu=(u,x,v,y)$ avec sig(u)=sig(v)
posons:
$K = S_{12} \times Z_2^{11} \times S_8 \times Z_3^7$
et considérons la fonction suivante:
$f: K \rightarrow \{-1,1\}$
$\mu = (u,x,v,y) \rightarrow f(\mu) = sig(u).sig(v)$
$|K| / |Ker(f)| = |Im(f)|$
or $sig(u) = sig(v) \Rightarrow f(\mu) = 1 \Rightarrow Ker(f) = G$
d'où
$|G| = |K|/2 = 12!.2^{11}.8!.3^7/2$ et ummuumumbalalala ....et hup !!!

$$|G| = \frac{12!\ 2^{12}\ 8!\ 3^{8}}{2\quad 3\quad 2} = 43\,252\,003\,274\,489\,856\,000$$

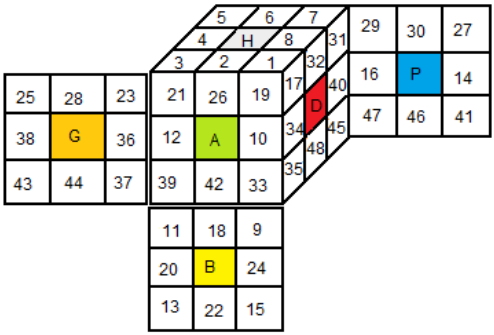
$$= 2^{27}3^{14}5^{3}7^{2}11$$

$$|G| = \frac{12!8!}{2}\ \frac{2^{12}}{2}\ \frac{3^{8}}{3} = \frac{|G^{+}|}{12}$$

$|G^{+}| = 12|G|$

NOTE : On a |G| - 1 = 43252003274489856000 - 1 = 43252003274489855999 est un nombre premier !!!, il est vraiment remarquable que |G| - 1 est premier car plus un nombre est grand moins il a de chance d'être premier !

La probabilité d'un nombre n soit un nombre premier est 1/ln(n) pour |G|-1 on a : 0,02 càd 2% de chance !! ce n'est pas beaucoup.



Les autocollants

Le GAP
Télécharger le GAP ici :

https://www.gap-system.org/Releases/4.4.12.html

https://fan2cube.fr/gap_rubikcube.txt:

Dans la fenêtre de cmd on se place dans le dossier de GAP
C:\Users\nom> cd\gap4r4\bin
C:\gap4r4\bin>gap < gap_rubikcube.txt

Le GAP nous donne bien
|G| = 43 252 003 274 489 856 000
$|G^+|$ = 519 024 039 293 878 272 000
$|G^+|/|G|$ = 12

```
gap> (1,3,5,7)(2,4,6,8)(17,21,25,29)(19,23,27,31)(26,28,30,32)
gap> (9,15,13,11)(18,24,22,20)(33,45,41,37)(35,47,43,39)(42,48,46,44)
gap> (1,35,11,23)(2,34,18,36)(3,17,9,37)(10,42,12,26)(19,33,39,21)
gap> (5,43,15,31)(6,38,22,40)(7,25,13,45)(14,46,16,30)(27,41,47,29)
gap> (3,39,13,27)(4,12,20,14)(5,21,11,41)(23,37,43,25)(28,36,44,38)
gap> (1,29,15,33)(7,47,9,19)(8,16,24,10)(17,31,45,35)(32,40,48,34)
gap> (2,26)
gap> (1,17,19)
gap> (2,8)(26,32)
gap> (10,36,14,40)(12,38,16,34)
gap> (2,30,22,42)(6,46,18,26)
gap> (4,32,24,44)(8,48,20,28)
gap> <permutation group with 9 generators>
gap> <permutation group with 6 generators>
gap> gap>
gap> |Lambda+| = 519024039293878272000
gap> |Lambda| = 43252003274489856000
gap> N = 12
gap> |G+| = 519024039293878272000
gap> |G| = |G+|/N = 43252003274489856000
gap> gap>
C:\GAP4R4\bin>
```

18 LES FACTEURS DE JORDAN-HOLDER DE G

Rappel: On dit qu'un groupe H est simple s'il ne possède pas des sous-groupes normaux (autre que 1 et H bien sûr). G n'est pas 'simple' du tout !!!!
Un groupe qui n'est pas simple est "fabriqué" en quelque sort, par des groupes simples!! comme un nombre est composé par des nombres premiers.
Précisons un peu plus:
Soit H un groupe non simple, alors il existe une suite (appelée de décomposition) de sous groupes
$H_0 = 1 \subset H_1 \subset H_2 \ldots \subset H_n = H$ avec H_{k-1} normal dans H_k , tel que
1. $H_k / H_{k-1} = L_k$ simple

Remarque:
- H_{k-1} doit être normal dans H_k, sinon on ne peut pas "diviser" les groupes !!!
- La condition: L_k est simple $\Leftrightarrow$ H_{k-1} est maximal

Les L_k sont des facteurs Jordan-Holder de H, qu'on notera $JH(H) = L_1.L_2....$
Note Le théorème de Jordan-Holder dit que toute suite de décomposition ayant la propriété 1. ci-dessus donne les même L_k, ce qui fait que H ne dépend pas des suites de décomposition mais seulement les L_k, les L_k sont donc les caractéristiques de H.

Exemple de groupes simples:
1. Groupe modulo: $\mathbb{Z}_p$ (p = premier) simple; en particulier $\mathbb{Z}_2$, $\mathbb{Z}_3$
2. Groupe Alterné: A_n (n>4) simple
et d'autres ....

Remarque
1. Si G_1,G_2 sont simples alors ⇒ on a : $JH(G_1 \times G_2) = G_1.G_2$
2. $JH(G) = JH(Ker(f)) . JH(Im(f))$ où f est un morphisme

On a posé:
$K = S_{12} \times Z_2^{11} \times S_8 \times Z_3^7$ mais on peut regrouper autrement par exemple
$= (S_{12} \times S_8) \times (Z_2^{11} \times Z_3^7)$ si on considère le morphisme g
$g: S_{12} \times S_8 \dashrightarrow \{-1,1\}$
$(u,v) \dashrightarrow g(u,v) = sig(u).sig(v)$ on voit que
$G = Ker(g) \times Z_2^{11} \times Z_3^7$et si on considère encore une autre morphisme h
$h: T \dashrightarrow \{-1,1\}$ avec $T = Ker(g)$
$(u,v) \dashrightarrow h(u,v) = sig(u)$ d'où $Ker(h) = A_{12} \times A_8$ finalement
$T/Ker(h) = Z_2 \Rightarrow Ker(g)/(A_{12} \times A_8) = Z_2$ on a alors une suite JH de Keg(g)
$\{id\} \subset A_{12} \subset A_{12} \times A_8 \subset Ker(g)$
D'où les facteurs JH de Ker(g) est
$JH(T) = A_{12}.A_8.Z_2$ (on peut dire aussi: JH(T) = JH(Ker(h)).JH(Im(h)))
et finalement les facteurs JH de G vaut

$JH(G) = A_{12}.A_8.Z_2^{12}.Z_3^7$ (G est fabriqué à partir de $A_{12}.A_8.Z_2^{12}.Z_3^7$)
d'où:

$$|G| = (12! \cdot 8! \cdot 2^{12} \cdot 3^{7})/4 = 43\,252\,003\,274\,489\,856\,000 = 2^{27}\,3^{14}\,5^{3}\,7^{2}\,11$$

Résumons:

1. Définition de G: G = l'ensemble des états produits par les rotations de base {H,B,A,P,G,D}.

2. $G \subset S_{12} \times Z_2^{12} \times S_8 \times Z_3^8$
(u,x,v,y) vérifiant
a. $\sum x_i = 0 \pmod 2$
b. $\sum y_i = 0 \pmod 3$
c. sig(u) = sig(v)

3. $G = Ker(g) \times Z_2^{11} \times Z_3^7$
où g: $S_{12} \times S_8$ -> {-1,1}
$(u,v) \rightarrow g(u,v) = sig(u).sig(v)$

4. Les facteurs de Jordan-Holder: $JH(G) = A_{12}.A_8.Z_2^{12}.Z_3^7$

5. $|G| = 12!\ 8!\ 2^{12}\ 3^8 / 2.2.3 = 43\,252\,003\,274\,489\,856\,000 = 2^{27}\,3^{14}\,5^{3}\,7^{2}\,11$

19 LE CENTRE DE G: Z(G)

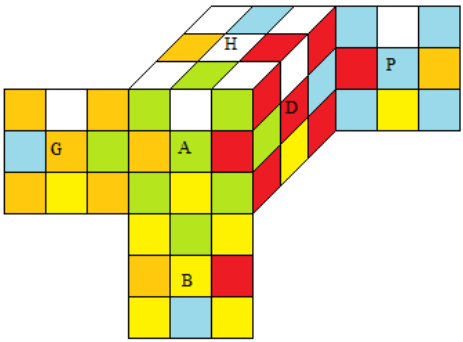
Le centre de G est des μ' tels que μμ' = μ'μ pour tout μ, on cherche donc μ' qui a ainsi cette propriété. Voyons donc un peu ce qui donne:

(u,x,v,y)(u',x',v',y') = (u',x',v',y')(u,x,v,y)
(uu',x+u(x'),vv',y+v(y')) = (u'u,x'+u'(x),v'v,y'+v'(y))
d'où:
uu' = u'u ∀u ⇒ dans S_{12} le seul élément qui commute avec tout le monde c'est u' = id (identité)

x + u(x') = x' + u'(x)
x - u'(x) = x' - u(x') comme c'est vrai pour tout x, on prend x = (0,0,0,0,0,0,0,0,0,0,0,0) d'où
x' = u(x') pour tout u, on cherche x' un vecteur qui soit invariant pour toutes les permutations, donc x' = (0,0,0,0,0,0,0,0,0,0,0,0) ou x' = (1,1,1,1,1,1,1,1,1,1,1,1) (on n'a pas d'autre choix pour x')
on fait exactement le même raisonnement pour v et y d'où
vv' = v'v ∀v ⇒ dans S_8 le seul élément qui commute avec tout le monde c'est v' = id (identité)
y - v'(y) = y' - v(y') comme c'est vrai pour tout y, on prend y = (0,0,0,0,0,0,0,0) d'où
y' = v(y') pour tout v donc y' = (0,0,0,0,0,0,0,0) ou y' = (1,1,1,1,1,1,1,1) ou encore y' = (2,2,2,2,2,2,2,2) (on n'a pas d'autre choix pour y')

et on doit avoir

$\sum x'_i = 0 \pmod 2 \Rightarrow x' = (0,0,0,0,0,0,0,0,0,0,0,0)$ ou $x' = (1,1,1,1,1,1,1,1,1,1,1,1)$ car $12 = 0 \pmod 2$
et
$\sum y'_i = 0 \pmod 3 \Rightarrow$ seul $y' = (0,0,0,0,0,0,0,0)$ convient car $y = (1,1,1,1,1,1,1,1) \Rightarrow 8 = 2 \pmod 3$ et $y = (2,2,2,2,2,2,2,2) \Rightarrow 16 = 1 \pmod 3$ ne conviennent pas
finalement on a 2 solutions:
$x' = (0,0,0,0,0,0,0,0,0,0,0,0)$, $y' = (0,0,0,0,0,0,0,0)$ ou $x' = (1,1,1,1,1,1,1,1)$, $y' = (0,0,0,0,0,0,0,0)$ c'est-à-dire $\mu' = (id,0,id,0)$ = e élément neutre du groupe G, et $\mu' = (id,1,id,0) = \varphi$ = SuperFlip (tout reste invariant, seules les arêtes changent de l'orientation)
$Z(G) = \{e, \varphi\}$ il n'y a que 2 éléments, en fait un seul élément φ car l'élément neutre e c'est évident qu'il est dans le centre.
et umumummuumbalallala et hop !!!!



$e \bullet \Phi = \varphi$
$\Phi = D'H^2PG'AH'PBAHB'GB^2A'DP'BA'H'P'HB'$ (Mike Reid par ordinateur)

Note:
En 1992 Dik T. Winter a trouvé une formule Φ du SuperFlip à 20f .
$\Phi = APH^2DA^2.D^2P^2H'BA.H^2D'G'HP^2.BD^2HP^2H$
$|\Phi| = 20f$ (face-rotation)
et (1995) Michael Reid démontre c'est le minimum pour la métrique face-rotation ($|A^2| = 1f$)

Michael Reid a trouvé (1995) une formule Φ du SuperFlip par ordinateur
$\Phi = D'H^2PG' .AH'PBA .HB'GB^2 .A'DP'BA' .H'P'HB'$
de longueur 24, $|\Phi| = 24$
et Jerry Bryan (1995) démontre que c'est la plus courte formule du SuperFlip $|\Phi| = 24$ pour la métrique quart-rotation ($|A^2| = 2$)
Résumons : SuperFlip φ : $|\Phi| = 24$, ou $|\Phi| = 20f$

20 LES QUATERNIONS

Vous arrivez ici, au pays des merveilles ...

On sait que le corps des nombres complexes $\mathbb{C}$ (dim = 2) correspond au plan $\mathbb{R}^2$. Un point (a,b) du plan $\mathbb{R}^2$ correspond au nombre complexe z:

$z = a+bi$ où $a,b \in \mathbb{R}$ avec la règle sur i: $i^2 = -1$

Hamilton voulait faire la même chose pour l'espace, c-à-d trouver un corps de dimension 3 correspond à l'espace $\mathbb{R}^3$. Un point (a,b,c) de l'espace $\mathbb{R}^3$ correspond au nombre q:

$q = a+bi+cj$ où $a,b,c \in \mathbb{R}$ avec les règles sur i,j à trouver.

Mais il n'a pas réussi[5]. En 1843 il a l'idée d'ajouter deux nombres j et k au lieu de j seulement, c-à-d

$q = a+bi+cj+dk$ où $a,b,c,d \in \mathbb{R}$ avec les règles sur i,j,k :

(20.1.1) $i^2 = j^2 = k^2 = ijk = -1$

Il trouva ainsi un corps non-commutatif à quatre dimensions ! correspond à l'espace $\mathbb{R}^4$.

Les règles sur i,j,k nous donnent la table de multiplication suivante:

---

[5] Théorème de Frobenius (1878): On ne peut construire un corps que sur $\mathbb{R}^2$ (c'est $\mathbb{C}$, les nombres complexes) et sur $\mathbb{R}^4$ (c'est $\mathbb{H}$, les quaternions)

x	i	j	k
i	-1	k	-j
j	-k	-1	i
k	j	-i	-1

Table de multiplication

ces nombre, nommés quaternions forment ainsi un corps non-commutatif $\mathbb{H}$ contenant $\mathbb{C}$.

$\mathbb{H} = \{q = a+bi+cj+dk \text{ avec } a,b,c,d \in \mathbb{R}\}$

Voyons comment on construit $\mathbb{H}$

$\mathbb{C}$: $z = a+bi$ où $a,b \in \mathbb{R}$, donc par analogie on prend

$\mathbb{H}$: $q = u+vj$ où $\underline{u,v \in \mathbb{C}}$ et j = nouveau nombre

$u = a + bi$

$v = c + di$

où $a,b,c,d \in \mathbb{R}$

$u+vj = a+bi+(c+di)j = a+bi+cj+dij$

donc si on pose $k = ij$ on aura

$q = a+bi+cj+dk \text{ avec } a,b,c,d \in \mathbb{R}$

Et les nombres i, j, k doivent suivre les règles (20.1.1)

Le nombre $i^2 = -1$ ok c'est un nombre complexe bien connu mais j et k ? (en fait il suffit de connaître j car $k = ij$)

concrètement on ne voit pas ce que sont les nombres j et k, en fait on peut définir les quaternions par des matrices 2x2 à coefficients complexes ou par des matrices 4x4 à coefficients réels .

Pour les nombres complexes on a:

$$\mathbb{C}: a + bi \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ; a, b \in \mathbb{R}$$

Pour les quaternions on prend :

$$\mathbb{H}: u + vj \to \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} ; u, v \in \mathbb{C}$$

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} = \begin{pmatrix} a & c \\ -c & a \end{pmatrix} + \begin{pmatrix} bi & di \\ di & -bi \end{pmatrix}$$

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

* en base à matrices complexes 2x2:

$$\iota = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \alpha = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

M = aι + bα + cβ + dγ avec a,b,c,d $\in \mathbb{R}$

et on a les relations (19.1.1) :

$\alpha^2 = \beta^2 = \gamma^2 = \alpha\beta\gamma = -\iota$

qui nous permettent de dire :

$\iota \to 1$, $\alpha \to i$, $\beta \to j$, $\gamma \to k$

Les α, β, γ relient aux matrices de Pauli ainsi:

$-i\alpha = \hat{\sigma}_z$, $i\beta = \hat{\sigma}_y$, $-i\gamma = \hat{\sigma}_x$.

* en base à matrices réelles 4x4:

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$M = aI + bA + cB + dC$ avec $a,b,c,d \in \mathbb{R}$

$$M = \begin{pmatrix} a & -b & c & -d \\ b & a & d & c \\ -c & -d & a & b \\ d & -c & -b & a \end{pmatrix} ; a,b,c,d \in \mathbb{R}$$

et on a les relations (19.1.1) :

$A^2 = B^2 = C^2 = ABC = -I$

qui nous permettent de dire :

$I \rightarrow 1$, $A \rightarrow i$, $B \rightarrow j$, $C \rightarrow k$

<u>Pour résumer</u> :

Pour les nombres complexes on a:

$$\mathbb{C}: a + bi \rightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ; a,b \in \mathbb{R}$$

Pour les quaternions on a:

$$\mathbb{H}: a + bi + cj + dk \rightarrow \begin{pmatrix} a & -b & c & -d \\ b & a & d & c \\ -c & -d & a & b \\ d & -c & -b & a \end{pmatrix} ; a, b, c, d \in \mathbb{R}$$

→ base {1,i,j,k}

$$\iota = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \alpha = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

→ base {ι,α,β,γ} matrices complexes 2x2

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

→ base {I,A,B,C} matrices réelles 4x4

20.2 LE GROUPE DES QUATERNIONS

On appelle le groupe des quaternions $(\mathbb{H}_8, .)$ c'est :

$\mathbb{H}_8 = \{ 1, i, j, k, -1, -i, -j, -k \}$

NOTE: Il y n'a que deux groupes non-abélien d'ordre 8: Le $\mathbb{H}_8$ et le groupe diédral D_4 . $\mathbb{H}_8$ est le seul groupe non-abélien d'ordre 8 à un seul élément d'ordre 2 (c'est -1).

Ne pas confondre entre le groupe des quaternions $(\mathbb{H}_8, .)$ et le corps des quaternions $(\mathbb{H},+, .)$

20.3 UN SOUS GROUPE INTÉRESSANT

La question est suivante:

Existe-t-il des états du Rubik's Cube qui représentent les nombres ?

La réponse est oui !!!

Intuitivement on peut penser que l'état résolu e représente le nombre 1, mais comment le justifier mathématiquement ?

En fait, on va montrer qu'il y a des états "exotiques" qui représentent des nombres, dont certains sont très célèbres !!

Commençons doucement ...

Soient $(\vartheta, .)$ un groupe et a,b deux éléments distingues de ϑ, vérifiant :

$$\begin{cases} a^4 = e\,,\ e = \text{élément neutre} \\ a^2 = b^2 \\ aba = b \end{cases}$$

on pose

$Q = \{e, a, b, ab, a^2, a^{-1}, b^{-1}, (ab)^{-1}\}$; a^{-1} = inverse de a.

et

$K = < a,b >$

alors $Q = K$

<u>Démonstration</u>

on pose $a^2 = \varepsilon$, $ab = c$.

$K \subset Q$, puisque K est le plus petit sous groupe contenant a,b . Il faut maintenant montrer qu'un élément de Q est dans K.

$e = a^4 \in K$

$a,b,\ c = ab \in K$

$\varepsilon = a^2 \in K$

$a^4 = e \Rightarrow a^{-1} = a^3 \in K$

$a^2 = b^2 \Rightarrow a^4 = b^4 \Rightarrow b^4 = e \Rightarrow b^{-1} = b^3 \in K$

$aba = b \Rightarrow abab = b^2 \Rightarrow c^2 = b^2 = a^2 \Rightarrow c^4 = e \Rightarrow c^{-1} = c^3 \in K$

donc $Q = K$.

$Q = \{e, a, b, ab, a^2, a^{-1}, b^{-1}, (ab)^{-1}\} = \{e, a, b, c, \varepsilon, \varepsilon a, \varepsilon b, \varepsilon c\}$

$a^4 = e \Rightarrow \varepsilon^2 = e$

$a^2a = aa^2 \Rightarrow \varepsilon a = a\varepsilon$

$b^2b = bb^2 \Rightarrow \varepsilon b = b\varepsilon$

$c^2c = cc^2 \Rightarrow \varepsilon c = c\varepsilon$

$a(\varepsilon b) = (a\varepsilon)b = (\varepsilon a)b = \varepsilon(ab)$

$(\varepsilon a)(\varepsilon b) = \varepsilon a\varepsilon b = \varepsilon^2 ab = eab = ab$

Les propriétés de ε montrent que ε se comporte comme "-1" dans $(\mathbb{Q},.)$ on pose donc

$\varepsilon = -e$ d'où

$a^2 = -e$

$\varepsilon a = (-e)a = -a$ (abrégé)

$\varepsilon b = (-e)b = -b$ (abrégé)

$\varepsilon c = (-e)c = -c$ (abrégé)

avec ces notations on a :

$Q = \{e, a, b, c, -e, -a, -b, -c\}$

Sans explication l'écriture -a (moins a) est choquante !! car dans $(\vartheta, .)$ on a l'opération "." et l'inverse x^{-1} et non opération "+" et -x (opposé)

Remarque : -a c'est aussi a^{-1}: $-a = a^{-1}$ de même $-b = b^{-1}$, $-c = c^{-1}$ mais $-e \neq e^{-1}$!!! $-e = \varepsilon = a^2$ est spécial (exotique)

$-e = a^2$
$-a = a^{-1} = a^3$
Théorème : Soit $(\vartheta, .)$ un groupe et soient a,b deux éléments distingues de ϑ vérifiant :

$$(*)\begin{cases} a^4 = e \\ a^2 = b^2 \\ aba = b \end{cases}$$

alors l'ensemble suivant:

$Q = \{e,a,b,ab,a^2,a^{-1},b^{-1},(ab)^{-1}\} = \{e, a,b,c,-e, -a,-b,-c\} = \langle a,b \rangle$
est isomorphe à
$\mathbb{H}_8 = \{ 1, i, j, k, -1, -i, -j, -k \}$
l'isomorphisme est donné par

$f : Q \rightarrow \mathbb{H}_8$

$f(a) = i$

$f(b) = j$

NOTE: On trouve Q aussi dans S_8

$a = (1,2,5,4)(3,8,6,7)$

$b = (1,8,5,7)(2,3,4,6)$

$Q = \langle a,b \rangle \subset S_8$

20.4 LES ÉTATS EXOTIQUES

On note 0 = (0,0,0, ... ,0) vecteur zéro

Soit maintenant les 2 états suivants :

a = (u,x,id,0) où u = (1,4)(2,3) et x = (1,0,1,0,0,0,0,0,0,0,0,0)
b = (p,z,id,0) où p = (1,2)(3,4) et z = (1,0,0,1,0,0,0,0,0,0,0,0)

Pour ne pas alourdir les écritures on prend seulement a et b la partie "arête-Haut": (u,x,id,0) ⇒ (u,x) avec x = (x_1,x_2,x_3,x_4)

$$a = \begin{pmatrix} u = (1,4)(2,3) \\ x = (1,01,0) \end{pmatrix}$$

$$b = \begin{pmatrix} p = (1,2)(3,4) \\ z = (1,0,0,1) \end{pmatrix}$$

$a^2 = (u,x)^2 = (u^2,x+u(x))$
détaillons pour le calcul a^2
¤ permutation: u^2 = id c'est clair
¤ orientation: x + u(x)
$x_1+x_4 = 1+0 = 1$
$x_2+x_3 = 0+1 = 1$
$x_3+x_2 = 1+0 = 1$
$x_4+x_1 = 0+1 = 1$
$a^2 = (id,\xi)$ où $\xi = (1,1,1,1)$

$$a^2 = \begin{pmatrix} id \\ (1,1,1,1) \end{pmatrix}$$

d'où
$a^4 = a^2\, a^2 = (id,\xi)(id,\xi) = (id,\xi+id(\xi)) = (id,\xi+\xi) = (id,0) = e$

$$a^4 = \begin{pmatrix} id \\ 0 \end{pmatrix}$$

→ $a^4 = e$ (état résolu)

On fait la même chose pour b
$b^2 = (p,z)^2 = (p^2, z+p(z))$
¤ permutation: $p^2 = id$
¤ orientation: z + p(z)
$z_1+z_2 = 1+0 = 1$
$z_2+z_1 = 0+1 = 1$
$z_3+z_4 = 0+1 = 1$
$z_4+z_3 = 1+0 = 1$
$b^2 = (id,\xi)$

→ $a^2 = b^2$
ab = (u,x)(p,z) = (up, x+u(z))

¤ permutation: up
up = (1,4)(2,3)(1,2)(3,4) = (1,3)(2,4)
¤ orientation: x' = x + u(z)
$x'_1 = x_1+z_4 = 1+1 = 0$
$x'_2 = x_2+z_3 = 0+0 = 0$
$x'_3 = x_3+z_2 = 1+0 = 1$
$x'_4 = x_4+z_1 = 0+1 = 1$
on pose
ab = c

$$c = \begin{pmatrix} (1,3)(2,4) \\ (0,0,1,1) \end{pmatrix}$$

aba = (up, x')(u,x) = (upu, x'+up(x))
¤ permutation: upu
upu = (1,3)(2,4)(1,4)(2,3) = (1,2)(3,4) = p
¤ orientation: x' + (up)(x)
$x'_1+x_3 = 0+1 = 1$
$x'_2+x_4 = 0+0 = 0$

$x'_3+x_1 = 1+1 = 0$
$x'_4+x_2 = 1+0 = 1$
aba = (p,z) = b (wwoaaowwww !!)

d'où
→ aba = b

a et b vérifient toutes les relations (*), donc
$Q = < a,b > = \{e, a, b, c, a^2, a^{-1}, b^{-1}, c^{-1}\} = \{e, a, b, c, a^2, a^3, b^3, c^3\}$
= {e, a, b, c, -e, -a, -b, -c}

Q = < a,b > est alors isomorphe à $\mathbb{H}_8$ avec isomorphisme f défini par

$f : Q \to \mathbb{H}_8$
f(a) = i
f(b) = j

$a \to i$
$a^2 \to i^2$ donc
-e → -1 c'est-à-dire l'état
$-e = \begin{pmatrix} id \\ (1,1,1,1) \end{pmatrix} \to -1$
-e → -1= les 4 arêtes-Haut sont flippées, le Miniflip

$a^4 = a^2\, a^2 = e \to (-1)(-1) = 1$ d'où
e → 1 ; l'état résolu e correspond bien au nombre 1

$a \to i$
$b \to j$
$ab = c \to ij = k$
$c \to k$

$a^4 = e \Rightarrow a^3 = a^{-1} \Rightarrow a^2 a = a^{-1}$

$a^2a = a^{-1} \rightarrow (-1)i$
$a^{-1} \rightarrow -i$
$a \rightarrow i$
$-a \rightarrow -i$
$Q = \{e, a, b, c, a^2, a^3, b^3, c^3\}$ où $c = ab$
$Q = \{e, a, b, c, -e, -a, -b, -c\} \rightarrow \{1, i, j, k, -1, -i, -j, -k\}$
Autrement dit le groupe du Rubik's Cube contient $\mathbb{H}_8$

$\mathbb{H}_8 = \{1, i, j, k, -1, -i, -j, -k\}$

Les états -e, $a^{-1} = a^3$, $b^{-1} = b^3$, $c^{-1} = c^3$, se nomment les états exotiques car c'est "l'opposé" de quelque chose e, a, b, c . Nul ne peut soupçonner que les motifs suivants représentent les nombres : l'entier -1, le nombre complexe i, le quaternion j ... !!!!

on pose :
C = D P' A D' P A' H P H P' A D' A' D' (minimale,14)
J = G' D P H' P' H G P G H G' P' D' H' (minimale,14)
K= P H G H^2 G' P' H' D' H^2 D (minimale, 12)
N = A' H' G' H P' H^2 P G H A H' D H^2 D' (minimale,16)

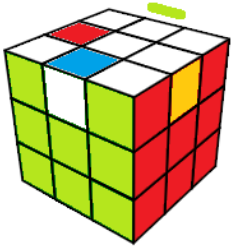
Remarque : Le programme Cube Explorer fournit la formule lorsqu'on lui donne le motif. C'est avec ce programme que j'ai pu trouver C et J pour a et b.

$i=e\bullet C$

$C=(HA,HD^{+})(HG^{+},HP)$

$j=e\bullet J$

$J=(HA,HG^{+})(HD,HP^{+})$



$k=e\bullet K$

$K=(HA^{+},HP)(HG^{+},HD)$

$-1=e \bullet N$

$N=(HA)^{+}(HD)^{+}(HP)^{+}(HG)^{+}$

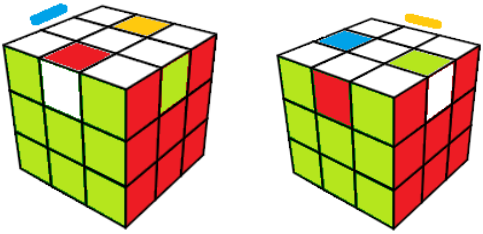
Le nombre complexe i, le quaternion j, le quaternion k et l 'entier -1,

Résumons :
On écrit seulement la partie d'arête-Haut
i = (u,x) où u = (1,4)(2,3) et x = (1,0,1,0)
j = (u,x) où u = (1,2)(3,4) et x = (1,0,0,1)
k = ij = (u,x) où u = (1,3)(2,4) et x = (0,0,1,1)

$i^2 = -1$ = (u,x) où u = id et x = (1,1,1,1) 4 arêtes-Haut flippées , MiniFlips

Note : on a: $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$ (- = flipper les arêtes)

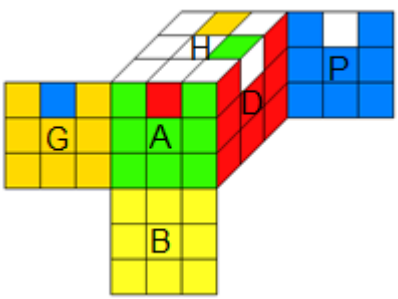
ij = -ji , jk = -kj, ki = -ik



i -i

Remarque important : Dans l'univers du Rubik's Cube il y a 3 antagonismes

Les formules V, les permutations σ, et les états μ. pour bien voir la différence de chaqu'un on va prendre un ex simple, par ex la configuration ci-dessous:



¤ La formule V = P' A D H' D' H P D P H P' D' A' H'

En regardant la formule, on ne voit pas comment sont disposées les pièces et leur orientation.

¤ La permutation σ = (HA,HD+)(HG,HP+)

La permutation nous dit :
→ (HA) permuté avec (HD) et le contenu de (HD) est pivoté

→ (HG) permuté avec (HP) et le contenu de (HP) est pivoté

on voit beaucoup mieux, mais impossible de savoir si une pièce est bien orientée ou pas avec ces notations (ces codages) !!!

¤ L'état μ

$$\mu = \begin{cases} u = (x_1, x_4)(x_2, x_3) \\ x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 0 \end{cases}$$

en abrégé

$$\mu = \begin{cases} u = (1,4)(2,3) \\ x = (1,1,0,0) \end{cases}$$

Avec les états on voit que x_3, x_4 sont bien orientées et on peut faire des calculs

(u,x)(u',x') = (uu',x+u(x'))

et savoir qui est bien orienté ou pas.

On voit bien le rôle différent de ces antagonismes.

20.5 LE SPIN D'ÉLECTRON

Le concept spin provient de la physique quantique, chaque particule possède un spin, par ex le photon a un spin 1, l'électron a un spin 1/2 ... Nous allons voir que certain état du Rubik's Cube représente le spin de l'électron !!

Soient 4 matrices déjà rencontrées à coefficients complexes suivantes:

$$\iota = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \alpha = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Le calcul nous montre que:

$\alpha^4 = \iota$

$\alpha^2 = \beta^2$

$\alpha\beta\ \alpha = \beta$

donc $\mathbb{H}_8$ vaut

$\mathbb{H}_8 = \{\iota, \alpha, \beta, \gamma, -\iota, -\alpha, -\beta, -\gamma\}$ où $\alpha\beta = \gamma$

Autrement dit on peut identifier

$\iota = 1, \alpha = i, \beta = j, \gamma = k$

D'autre part les matrices de Pauli valent:

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et le spin $\hat{S}_z$ de l'électron suivant z est

$$\hat{S}_z = \frac{\hbar}{2}\hat{\sigma}_z$$

$$\hat{S}_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\hat{S}_z = -i\frac{\hbar}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -i\frac{\hbar}{2}\alpha = \frac{\hbar}{2i}\alpha$$

de même pour y, x

$$\hat{S}_z = \frac{\hbar}{2i}\alpha, \qquad \hat{S}_y = \frac{\hbar}{2i}\beta, \qquad \hat{S}_x = \frac{\hbar}{2i}\gamma$$

Comme on connaît α on connaîtra $\hat{S}_z$, β→ $\hat{S}_y$, ... donc les états suivants représentent le spin de l'électron suivant l'axe .

représente le spin de l'électron suivant z (α⇔i)

représente le spin de l'électron suivant y (β⇔j)

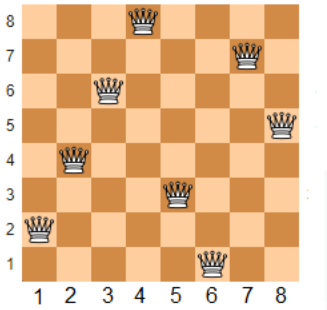
représente le spin de l'électron suivant x (γ⇔k)

C'est étonnant n'est ce pas ??

20.6 PROBLÈME DES 8 REINES

Le problème des 8 Reines en échec est le suivant:

Comment placer les 8 reines sur l'échiquier sans qu'elles se menacent mutuellement ? voici une solution

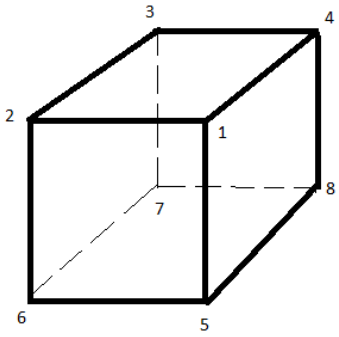


Soit V la formule suivante:

$V = A^2HP^2\ HD^2A^2\ D^2HP^2\ BHG^2B'\ A^2H^2$

l'interprétation de cette formule est suivante:

Si on note les sommets du Rubik's Cube comme indique la fig ci-dessous.



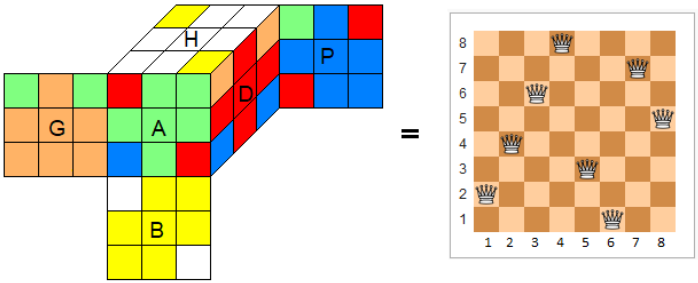
En appliquant la formule on voit que les sommets fait un 7-cycle

p = (1,2,4,8,5,3,6) en écrivant comme une permutation des sommets ça nous donne

p(1) = 2, p(2) = 4, p(3) = 6, p(4) = 8, ...

p = [2,4,6,8,3,1,7,5] le nombre 24683175 est une solution du problème des 8 reines !!!!

1er reine en position 2
2ème reine en position 4
3ème reine en position 6
etc ...



Il y a une connexion entre le Rubik's Cube et le jeu d'échec !!!

Qui peut imaginer que cet état du Rubik représente une solution des 8 reines ?...

21 DROITE PROJECTIVE F_5

On rappelle que la droite projective de F_5 est:
$\overline{F_5}$ = { 0,1,2,3,4,∞ } en plus les opérations dans F_5 on ajoute les opérations suivantes:

$$\frac{1}{0} = \infty \; ; \; \frac{1}{\infty} = 0$$

ou encore 0 x ∞ = ∞ x 0 = 1 et on peut dresser les tables '+' et 'x' de $\overline{F_5}$

+	0	1	2	3	4	∞
0	0	1	2	3	4	∞
1	1	2	3	4	0	∞
2	2	3	4	0	1	∞
3	3	4	0	1	2	∞
4	4	0	1	2	3	∞
∞	∞	∞	∞	∞	∞	∞

addition

Remarque : '∞' n'est qu'un symbole on peut le noter par n'importe quel caractère par ex 'Ω' dans ce cas les opérations sera :

1/Ω = 0, 1/0 = Ω, 4+Ω = Ω, 0xΩ = Ωx0 = Ω, ... etc ...

X	0	1	2	3	4	∞
0	0	0	0	0	0	1
1	0	1	2	3	4	∞
2	0	2	4	1	3	∞
3	0	3	1	4	2	∞
4	0	4	3	2	1	∞
∞	1	∞	∞	∞	∞	∞

multiplication

On définit alors 2 fonctions suivantes sur $\overline{F}_5$:

$f : \overline{F}_5 \rightarrow \overline{F}_5$

$$f(x) = \frac{x+4}{x+1}$$

$g : \overline{F}_5 \rightarrow \overline{F}_5$

$g(x) = 3x + 3$

et

calculons les valeurs des ces fonctions (n'oubliez pas qu'on est dans $\overline{F}_5$ càd mod 5)

$f(0) = 4$

$f(1) = 0 \pmod 5$

$f(2) = 6/3 = 2$

$f(3) = 7/4 = 2/4 = 1/2 = 3$ ($2.3 = 6 = 1 \pmod 5$, donc 3 est l'inverse de 2)

f(4) = 8/5 = 3/0 = ∞

$$f(x) = \frac{x(1+\frac{4}{x})}{x(1+\frac{1}{x})} = \frac{(1+\frac{4}{x})}{(1+\frac{1}{x})}$$

$$f(\infty) = \frac{(1+\frac{4}{\infty})}{(1+\frac{1}{\infty})} = 1$$

x = 0, 1, 2, 3, 4, ∞
f(x) = 4, 0, 2, 3,∞,1
et pour la fonction g(x)
g(0) = 3
g(1) = 3.1+3 = 6 = 1 (mod 5), on est dans $\overline{F}_5$
g(2) = 3.2+3 = 9 = 4 (mod 5)
g(3) = 3.3+3 = 12 = 2 (mod 5)
g(4) = 3.4+3 = 15 = 0 (mod 5)
g(∞) = 3.∞+3 = ∞

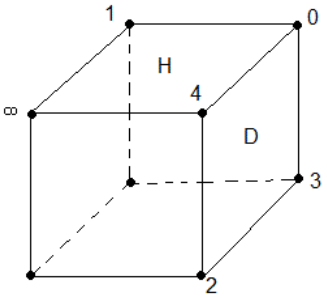
x = 0, 1, 2, 3, 4, ∞
g(x) = 3, 1, 4, 2, 0, ∞

On associe f(x) comme la rotation H et g(x) à la rotation D et voyons comment placer les éléments de $\overline{F}_5$ sur le Cube.

On a f(2) = 2, f(3) = 3 ça signifie que 2, 3 ne sont pas perturbés par la rotation H, donc ils sont sur Bas-Droite
On a g(1) = 1, g(∞) = ∞ ça signifie que 1, ∞ ne sont pas perturbés par la rotation D, donc ils sont sur Haut-Gauche
Donc 0, et 4 sur Haut-Droite.
* 1, ∞ sur Haut-Gauche et f(∞) =1 ⇒ (HAG) =∞⇒(HGP) = 1
* 0, 4 sur Haut-Droite et f(1) = 0 ⇒ (HPD) = 0 ⇒ (HDA) = 4

* 2, 3 sur Bas-Droite et g(0) = 3 ⇒ (BDP) = 3 ⇒ (BAD) = 2

Ainsi les éléments de $\overline{F}_5$ sont sur les sommets (on ignore les orientations) comme indique la fig ci-dessous



(HAG) = ∞ et (HPD) = 0

Observons bien, f(x) agit exactement comme la rotation H agit sur les sommets du Rubik's Cube !!! g(x) aussi , elle agit exactement comme la rotation D agit sur les sommets !!! ce n'est pas merveilleux ça ? on peut regarder l'effet de H et D sur les sommets comme des fonctions homographiques sur $\overline{F}_5$ ou des matrices !!!

$$H \dashrightarrow f(x) = \frac{x+4}{x+1}$$

D → g(x) = 3x + 3

$$T = \begin{pmatrix} 1 & 4 \\ 1 & 1 \end{pmatrix} ; Q = \begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}$$

p = (0,4,∞,1) permutation associée à la rotation H
q = (0,3,2,4) permutation associée à la rotation D
comment pourrait-on soupçonner que l'emplacement (HAG) représente ∞ : (HAG) = ∞ et (HPD) = 0 !!!

22 LE GROUPE < H,D >

Rappels :

$$f(x) = \frac{x+4}{x+1}$$

$g(x) = 3x + 3$

$GL(n,p) = \{\text{Matrice nxn à coef dans } F_p \text{ , det} \neq 0\}$

$SL(n,p) = \{\text{Matrice nxn à coef dans } F_p \text{ , det} = 1\}$

$ZG(n,p)$ centre de $GL(n,p)$ = matrice aI , $a \in F_p$ $a \neq 0$

$ZS(n,p)$ centre de $SL(n,p)$ = matrice aI , $a \in F_p$ $a^n = 1$

$PGL(n,p) = GL(n,p)/ZG(n,p)$

$PSL(n,p) = SL(n,p)/ZS(n,p)$

Les formules :

¤ $|GL(n,p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1})$

$|SL(n,p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) / (p-1)$

$|PGL(n,p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) / (p-1)$

$|PSL(n,p)| =$

$= (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) / (p-1)\text{pgcd}(n,p-1)$

Voyons ce que c'est le groupe engendré par deux rotations adjacentes comme H,D.

Soit

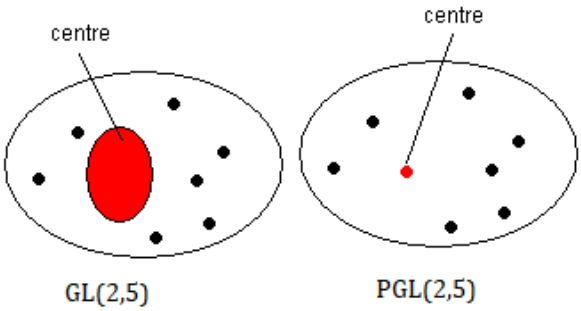
$GL(2,5) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} a,b,c,d \in F_5 \mid ad-cb \neq 0 \}$

et son centre

$ZG(2,5) = \{\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} k \in F_5 \mid k \neq 0 \} = F_5^*$

$PGL(2,5) = GL(2,5)/ZG(2,5)$

En gros, ça signifie que dans GL(2,5) on a comprimé le centre en un point!



cela veut dire aussi qu'on considère les multiples (par un scalaire k≠0) sont les même:
comme pour les fractions on a 1/7 = 2/14 = 3/21 ...
puis
$SL(2,5) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a,b,c,d $\in F_5$ | ad-cb = 1 }
et son centre

$ZS(2,5) = \{\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$ $k \in F_5$ | $k^2 = 1$ }
PSL(2,5) = SL(2,5)/ZS(2,5)

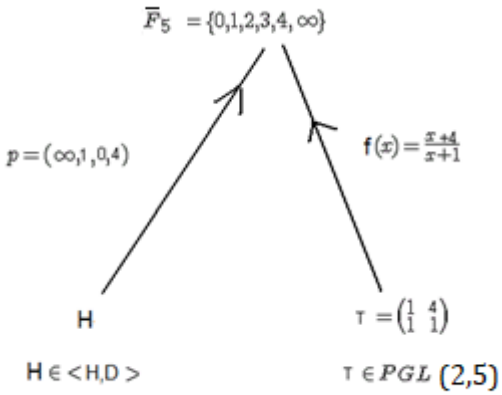
¤ $|GL(2,p)| = (p^2-1)(p^2-p)$

$|SL(2,p)| = (p^2-1)(p^2-p)/(p-1)$

$|PGL(2,p)| = (p^2-1)(p^2-p)/(p-1)$

$|PSL(2,p)| = (p^2-1)(p^2-p)/(p-1)pgcd(2,p-1)$

Soit K un sous groupe de M. Les formules génèrent des permutations sur les sommets et arêtes (on ignore les orientations), K génère donc en deux sous groupes: un sous groupe de S_8 (pour les sommets) qu'on va noter K_s , et un sous groupe de S_{12} (pour les arêtes) qu'on notera K_a.
Considérons maintenant le sous-groupe < H,D > de M, engendré par les rotations H et D. Le but de ce paragraphe est de démontrer que
$< H,D >_s = PGL(2,5)$ (D. SINGMASTER)
$< H,D >_a = S_7$ (D. SINGMASTER)



1. La rotation H ordonne à p (permutation) de bouger les éléments de $\overline{F}_5$
2. La matrice T ordonne à f(x) (fonction) de bouger les éléments de $\overline{F}_5$

Lorsqu'on fait une rotation H ou D , on permute les sommets (par p ou q) comme les fonctions f(x) et g(x) agissent sur les sommets , Mais les fonctions f(x) et g(x) ne sont rien d'autres que les matrices T et Q. On a donc:
$< H,D >_s = < p,q > = < T,Q >$
<u>Quelques rappels</u>
On sait que:
1. $|PGL(2,5)| = 5(5^2-1) = 120$ et
$|PSL(2,5)| = 5(5^2-1)/pgcd(2,5-1) = 60$
2. PSL(2,5) est engendré par les matrices de transvections(°)

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \neq 0 \in F_5$

(°)NOTE: définition de la matrice de tranvection: c'est une matrice dont 1 sur le diagonale, un seul a≠0 quelque part et 0 ailleurs, par ex:

$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix} \ldots$

Démonstration :
I. < T,Q > ⊂ PGL(2,5) évident
II. PSL(2,5) ⊂ < T,Q >
Pour cela il suffit d'exprimer les matrices
$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$
en fonction de T et Q

On rappelle que dans PGL(2,5) on a
$\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 5$
Montrons d'abord :
$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^a$ et $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^a$
on va montrer par récurrence:
pour a = 1 , c'est vrai
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^1$
Supposons que la formule soit vraie pour a,
$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^a$ (HR)
et montrons qu'elle reste encore vraie pour (a+1)
Allons y

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}^{a+1} = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}^{a}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} \underset{HR}{=} \begin{pmatrix}1 & a\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$$
$$= \begin{pmatrix}1 & a+1\\0 & 1\end{pmatrix}$$

La formule est ainsi démontrée, on fait de même pour l'autre matrice.
Essayons maintenant exprimer les matrices
$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}$
en fonction de T, Q

Allons-y

$$T^2 = \begin{pmatrix}1 & 4\\1 & 1\end{pmatrix}\begin{pmatrix}1 & 4\\1 & 1\end{pmatrix} = \begin{pmatrix}5 & 8\\2 & 5\end{pmatrix} = \begin{pmatrix}0 & 3\\2 & 0\end{pmatrix} \pmod 5$$
$$T^{-2} = \begin{pmatrix}0 & -3\\-2 & 0\end{pmatrix} = \begin{pmatrix}0 & 2\\3 & 0\end{pmatrix} \pmod 5$$

$$Q^3 = \begin{pmatrix}2 & 0\\1 & 1\end{pmatrix}$$
$$TQ^3 = \begin{pmatrix}2 & 0\\2 & 2\end{pmatrix} = \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}$$
$$T^2\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}T^{-2} =$$

$$= \begin{pmatrix}0 & 3\\2 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}0 & 2\\3 & 0\end{pmatrix} = \begin{pmatrix}3 & 3\\2 & 0\end{pmatrix}\begin{pmatrix}0 & 2\\3 & 0\end{pmatrix} = \begin{pmatrix}9 & 6\\0 & 4\end{pmatrix}$$

$$= \begin{pmatrix}4 & 1\\0 & 4\end{pmatrix} = 4\begin{pmatrix}1 & 4\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 4\\0 & 1\end{pmatrix}$$
$$T^2\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}T^{-2} = \begin{pmatrix}1 & 4\\0 & 1\end{pmatrix} = K$$
$$K^9 = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$$

ça y est on a gagné car les matrices

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^a$ et $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^a$
s'expriment en fonctions de T et Q

III. On a : PSL(2,5) ⊂ < T,Q > ⊂ PGL(2,5)
on sait que entre PSL(2,5) et PGL(2,5) il n' a rien (car l'indice = 2), donc soit < T,Q > = PGL(2,5) soit < T,Q > = PSL(2,5)
pour montrer que < T,Q > ≠ PSL(2,5) il suffit de trouver un élément de < T,Q > et qui n'est pas dans PSL(2,5). Prenons T par exemple, on a det(T) = 1- 4 = -3 = 2 (mod 5)
et sous sa forme générale det(T) = $2.k^2$ (on n'a pas simplifié la fraction f(x) par k)
si T ∈PSL(2,5) det(T)=1 ⇒ $2k^2 = 1 \Rightarrow k^2 = 1/2 = 3$ (mod 5)
impossible, car les carrés dans F_5 sont :
$0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 4$, $4^2 = 16 = 1$ (mod 5)
il n'y a pas de k^2 qui vaut 3 dans F_5, donc T n'est pas dans PSL(2,5) on a forcement
< T,Q > = PGL(2,5)

Et voila .....

$< H,D >_s$ = PGL(2,5) (D. SINGMASTER)

On a $< H,D >_a \subset S_7$, pour montrer $< H,D >_a = S_7$, analysons un peu la situation :
* Les sommets et les arêtes sont en phase (loi de parité)
* H, D ne renversent pas les arêtes, donc $\mathbb{Z}_2$ n'intervient pas,
* L'orientation des sommets est fixé dès qu'il y a 5 sommets bien orientés (loi des twists).
* $< H,D > = < H,D >_a$ x PGL(2,5)/2 x $3^6/3$
D'autre part le programme GAP (.::download GAP ici::.),

nous donne le cardinal de
$|< H,D >| = 73483200$ finalement nous avons
$|< H,D >_a| = w$
$|PGL(2,5)| = 120$

$$|< H,D >| = 73483200 = \frac{w.120}{2}\frac{3^6}{3}$$

On divise par 2 (arêtes, sommets en phase) et 3 (loi des twists) .

(Rappelez vous pour |G|

$$|G| = \frac{12!.8!}{2}\frac{3^8}{3}\frac{2^{12}}{2}$$

on divise par 2 à cause de la loi de parité: sig(u) = sig(v)
on divise par 3 à cause de la loi des twists: $\sum y_i = 0 \pmod 3$
on divise par 2 à cause de la loi des flips: $\sum x_i = 0 \pmod 2$)

d'où
$w = (73483200 \times 6)/(120 \times 729) = 5040 = 7! = |S_7|$ d'où

$< H,D >_a = S_7$ (D. SINGMASTER)

on a donc:
$< H,D > = S_7 \times PGL(2,5) \times \mathbb{Z}_3^6 /(2x3)$ et on a bien

$$| < H,D > | = \frac{7!.120}{2}\frac{3^6}{3} = 73483200$$

23 LE GROUPE CROISÉ DU RUBIK'S CUBE < XY' >

On sait qu'il existe un seul groupe simple GS_{168} non-abélien à 168 éléments. C'est le deuxième groupe simple, après le groupe alterné A_5. Le GS_{168} est vraiment extraordinaire car on le trouve pratiquement partout .....

- La quartique de Klein:
E: $x^3y + y^3z + z^3x = 0$; $x,y,z \in \mathbb{C}$. Le groupe des automorphismes qui laissent invariant E est GS_{168}
Aut-inv(E) = GS_{168}

- L'équation de degré 7:
$P(x) = x^7 - 7x + 3 = 0$ Le groupe de Galois de P, est GS_{168}
Gal(P) = GS_{168}

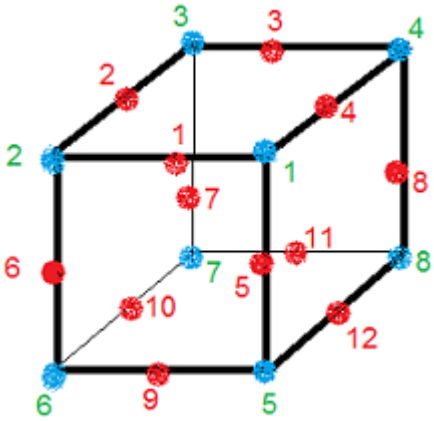
- Dans A_7:
a = (1,2,4)(3,5,6) ; # a = (1,2,3,4,5,6,7)
b = (1,7)(2,6) ; # b = (1,2)(3,6)
<a,b> = GS_{168}

- Groupe des matrices:
GL(3,2) = GS_{168}

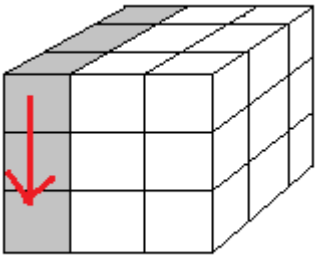
- Projective:
PSL(3,2) = GS_{168}

et ... et .... vous avez deviné ... il se trouve aussi dans le Rubik's Cube !!!!!

Dans ce chapitre on ne considère que les pièces, c'est-à-dire on ignore les orientations , les sommets et les arêtes sont alors identifiés par un numéro.



Les sommets et les arêtes sont numérotés



Rotation croisée G

Définition une rotation croisée : Une rotation croisée c'est une rotation par rapport aux sommets ou par rapport aux faces et qui déplace les pièces sommets et arêtes. Dans le cas du Rubik's Cube c'est simplement une rotation de base {H,B,A,P,G,D} , (pour le Pyraminx , une rotation croisée n'est pas une rotation de base).

On pose:

¤ K_s = K = < XY' | X,Y ∈{H,B,A,P,G,D}, pour les sommets >
K engendre un groupe de permutations des sommets C , par définition C est le groupe Croisé du Rubik's Cube .

¤ K_a = < XY' | X,Y ∈{H,B,A,P,G,D} , pour les arêtes >
K_a engendre un groupe de permutations des arêtes C_a , par définition C_a est le groupe Croisé des arêtes du Rubik's Cube .

Voici un script en GAP qui permet de calculer le groupe Croisé C du Rubik's Cube et le groupe Croisé des arêtes C_a.

https://www.gap-system.org/Releases/4.4.12.html

```
# Cross = < XY' | X,Y rotations croisées >

# (Cube : F=6,S=8,A=12)

# 3  3  4

# 2  H  4

# 2  1  1

# -------
```

```
# 6  A  5|7 P  8
# -------
# 7  11 8
# 10 B  12
# 6  9  5

# le groupe Croisé du Rubik's Cube (Croisé sommet)
vH := (1,2,3,4) ;
vB := (5,8,7,6) ;
vA := (1,5,6,2) ;
vP := (4,3,7,8) ;
vG := (2,6,7,3) ;
vD := (1,4,8,5) ;
SX := [vH, vB, vA, vP, vG, vD];
SYp := [vH^-1, vB^-1, vA^-1, vP^-1, vG^-1, vD^-1 ] ;
SXtxt := ['H', 'B', 'A', 'P', 'G', 'D'];
SYptxt := ['h', 'b', 'a', 'p', 'g', 'd'] ;

# le groupe Croisé des arêtes (Croisé arête)
```

```
uH := (1,2,3,4);

uB := (9,12,11,10);

uA := (1,5,9,6);

uP := (3,7,11,8);

uG := (2,6,10,7);

uD := (5,4,8,12) ;

AX := [uH, uB, uA, uP, uG, uD];

AYp := [uH^-1, uB^-1, uA^-1, uP^-1, uG^-1, uD^-1 ] ;



# donne une formule-croisée de longueur 2n

RandomCrossFormula := function(n)

 local nombre, permutations, k , formule, m ;

 nombre := List([1..n], i -> RandomList([1..6])); #[1..6] ==>
6 rotations

 permutations := [];

 formule := [];


 for k in nombre do
```

```
                Append(permutations,[SX[k]]);
                Append(formule,[SXtxt[k]]);

                m :=  RandomList([1..6]);
                while k=m do
        m :=  RandomList([1..6]);
    od;

            Append(permutations, [SYp[m]]);
        Append(formule,[SYptxt[m]]);

od;

Product(permutations);

formule := ReplacedString( formule, "h", "H'" );;
formule := ReplacedString( formule, "b", "B'" );;
formule := ReplacedString( formule, "a", "A'" );;
```

```
 formule := ReplacedString( formule, "p", "P'" );;

 formule := ReplacedString( formule, "g", "G'" );;

 formule := ReplacedString( formule, "d", "D'" );;


 return formule;

end;


#Print("\n ", RandomCrossFormula(5) , "\n" );


generators := Set(Arrangements([1..6],2), t -> SX[t[2]] *
SYp[t[1]]);; #[1..6] ==> 6 rotations

Cross := Group(generators);;

Size(Cross) ;

IsSimpleGroup( Cross ) ;

Print("\n Cross = ", StructureDescription(Cross) , "\n" );


generators := Set(Arrangements([1..6],2), t -> AX[t[2]] *
AYp[t[1]]);; #[1..6] ==> 6 rotations

Cross := Group(generators);;
```

Print("\n Cross-edge = ", StructureDescription(Cross) , "\n");

```
gap> gap> gap> gap> gap> gap> 168
gap> true
gap>
 Cross = PSL(3,2)
gap> gap> gap> gap>
 Cross-edge = A12
gap> gap>
C:\GAP4R4\bin>
```

le GAP calcule le cardinal de ce groupe et nous fournit un joli nombre:
|C| = 168 éléments (et identifie ce groupe comme PSL(3,2) = PSL(2,7))

et $C_a = A_{12}$

Comme dans le chapitre précédent, la droite projective de F_7 est définie par:
$\overline{F}_7$ = { 0,1,2,3,4,5,6,∞ } en plus les opérations dans F_7 on ajoute comme d'habitude les deux opérations suivantes:

$$\frac{1}{0} = \infty \; ; \; \frac{1}{\infty} = 0$$

ou encore 0 x ∞ = ∞ x 0 = 1
On peut dresser les tables '+' et 'x' de $\overline{F}_7$ comme ça les opérations serons plus claires

+	0	1	2	3	4	5	6	∞
0	0	1	2	3	4	5	6	∞
1	1	2	3	4	5	6	0	∞
2	2	3	4	5	6	0	1	∞
3	3	4	5	6	0	1	2	∞
4	4	5	6	0	1	2	3	∞
5	5	6	0	1	2	3	4	∞
6	6	0	1	2	3	4	5	∞
∞	∞	∞	∞	∞	∞	∞	∞	∞

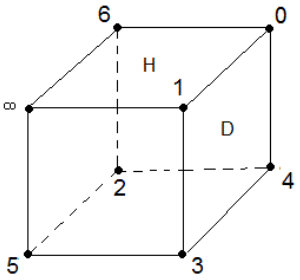
Addition

X	0	1	2	3	4	5	6	∞
0	0	0	0	0	0	0	0	1
1	0	1	2	3	4	5	6	∞
2	0	2	4	6	1	3	5	∞
3	0	3	6	2	5	1	4	∞
4	0	4	1	5	2	6	3	∞
5	0	5	3	1	6	4	2	∞
6	0	6	5	4	3	2	1	∞
∞	1	∞	∞	∞	∞	∞	∞	∞

Multiplication

On sait que (HAG) = ∞ et (HPD) = 0 , plaçons maintenant les éléments de $\overline{F}_7$ sur les sommets du Rubik's Cube de la façon suivante:

A→(∞,1,3,5) et P→(0,6,2,4) permutation associées comme la fig ci-dessous



(HAG) = ∞ et (HPD) = 0

On définit ensuite 3 fonctions suivantes sur $\overline{F}_7$

f : $\overline{F}_7 \rightarrow \overline{F}_7$

f(x) = 2x

g : $\overline{F}_7 \rightarrow \overline{F}_7$

g(x) = 2x + 1

et

h : $\overline{F}_7 \rightarrow \overline{F}_7$

$$h(x) = -\frac{1}{x}$$

calculons les valeurs des ces fonctions (n'oubliez pas qu'on est dans $\overline{F}_7$, càd modulo 7)

x = 0, 1, 2, 3 ,4, 5, 6, ∞
f(x) = 0, 2, 4, 6, 1, 3, 5, ∞

x = 0, 1, 2, 3 ,4, 5, 6, ∞
g(x) = 1, 3, 5, 0, 2, 4, 6, ∞

x = 0, 1, 2, 3 ,4, 5, 6, ∞
h(x) = ∞, -1, -1/2, -1/3, -1/4, -1/5, -1/6, 0
h(x) = ∞, 6, -4, -5, -2, -3, -6, 0
h(x) = ∞, 6, 3, 2, 5, 4, 1, 0

Prenons les 3 formules suivantes:
AB'GA' → m permutation associée
x = 0, 1, 2, 3 ,4, 5, 6, ∞
A = 0, 3, 2, 5, 4, ∞, 6, 1
AB' = 0, 5, 4, 2, 3, ∞, 6, 1
AB'G = 0, 2, 4, 6, 3, 5, ∞, 1
AB'GA' = 0, 2, 4, 6, 1, 3, 5, ∞ → m = (1,2,4)(3,6,5)

BD' → n
x = 0, 1, 2, 3, 4, 5, 6, ∞
B = 0, 1, 5, 4, 2, 3, 6, ∞
BD' = 1, 3, 5, 0, 2, 4, 6, ∞ → n = (0,1,3)(2,5,4)
BH'BH' → q
x = 0, 1, 2, 3 ,4, 5, 6, ∞
BH'BH' = ∞, 6, 3, 2, 5, 4, 1, 0 → q = (0,∞)(1,6)(2,3)(4,5)

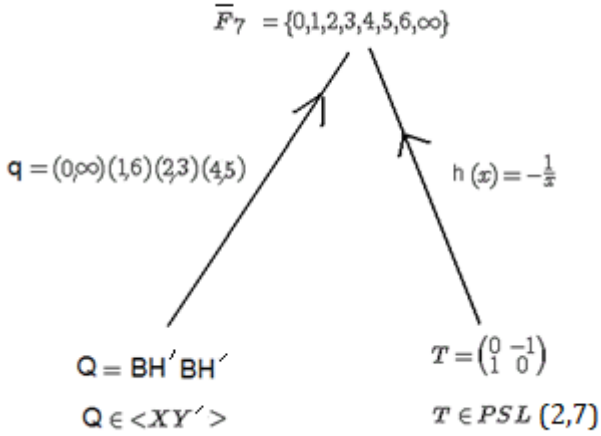
m fait exactement la même chose que f(x), de même pour g(x)⇔n, h(x)⇔q

Les 3 fonctions ci-dessus fournissent les 3 matrices de déterminant = 1 à coefficients dans F_7

$W = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 5 \end{pmatrix}$ det(W) = 50 = 1 mod (7)

$S = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 5 \\ 0 & 5 \end{pmatrix}$ det(S) = 50 = 1 mod (7)

$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ det(T) = 1



1. La formule Q ordonne à q (permutation) de bouger les éléments de $\overline{F}_7$
2. La matrice T ordonne à h(x) (fonction) de bouger les éléments de $\overline{F}_7$

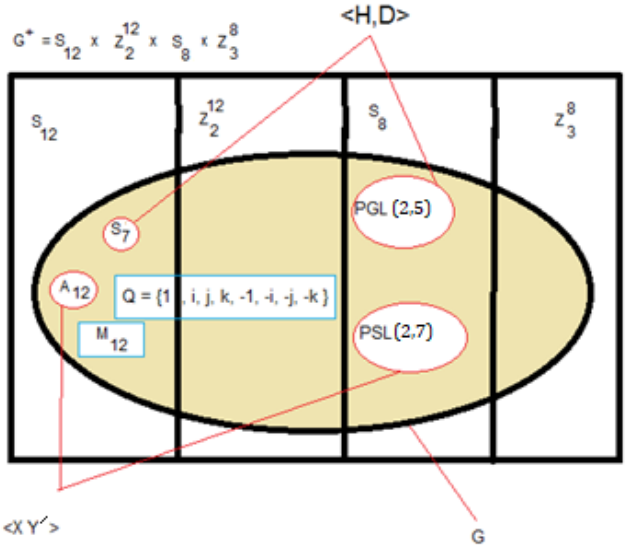
On démontre que m, n, q engendrent C et W, S, T engendrent PSL(2,7)
on définit maintenant la fonction z:
z : C → PSL(2,7)
de façon suivante:
z(m) = W , z(n) = S et z(q) = T
si c'est m, je dis que ça vaut W, si c'est n, je dis que ça vaut S, ...
d'où
u = mnq → z(u) = WST
a). Montrons d'abord que c'est bien un homomorphisme
En effet un élément de C s'écrit comme un produit des

m,n,q par exemple
$v = m^2qn^3$ et par définition on a
$z(m^2qn^3) = W^2TS^3$ qui vaut
$= z(m)^2z(q)z(n)^3$ = c'est bien un homomorphisme

b). z est évidement surjectif : en effet, un élément de PSL(2,7) s'écrit comme un produit des W,S,T par exemple
$K = T^2W^2S^4 = z(q)^2z(m)^2z(n)^4 = z(q^2m^2n^4)$

mais $|PSL(2,7)| = 7(7^2-1)/pgcd(2,7-1) = 168$
$|C| = |PSL(2,7)|$, donc z est bijectif !!!! on a bien un bel isomorphisme entre C et PSL(2,7)

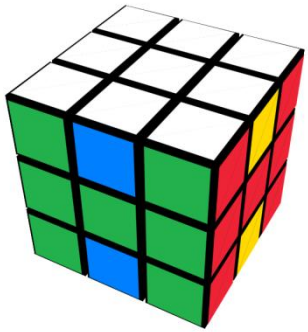
$C = PSL(2,7) = GS_{168}$



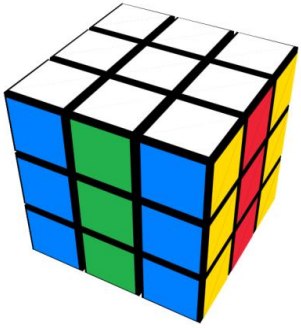
Remarque : le GAP mous montre que $C_a = A_{12}$

24 LES JOLIS MOTIFS

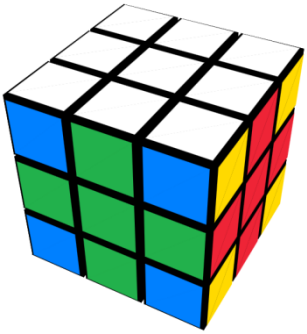
Dans ce chapitre on a une collections de jolis motifs



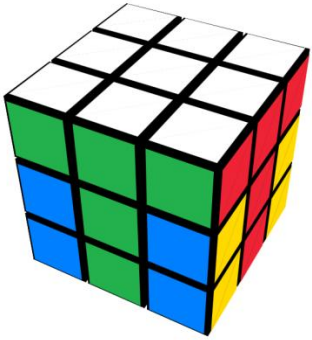
$4H = H^2D^2G^2A^2\ P^2H^2D^2G^2\ A^2P^2$



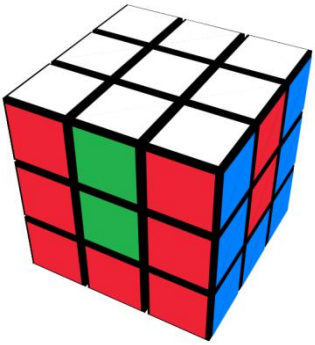
$4I = (A^2D^2P^2)^2$



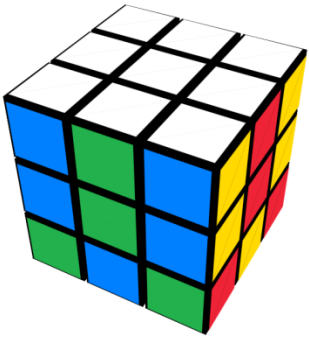
4Plus = $HA^2D^2A^2$ $H'BG^2$ P^2G^2B'



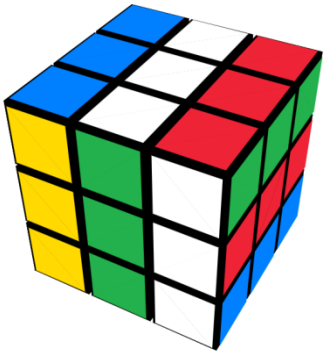
4T = $DGH^2D'G'APH^2A'P'H^2$



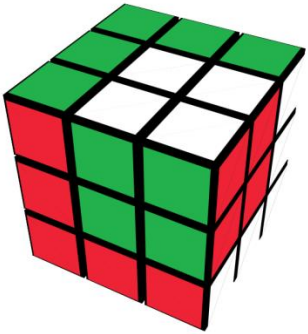
$4U = AD'P'B^2G'\ HB'P\ B^2DAG'$



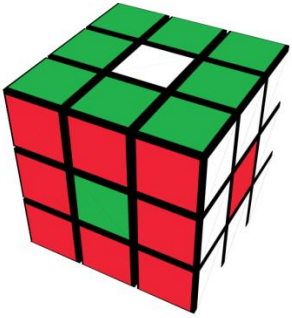
$4Y = (D^2A^2G^2)^2\ B^2$



6Drapeaux = GHA^{2}DG' H^{2}P'HB P^{2}GAP' D'GA' DG'D

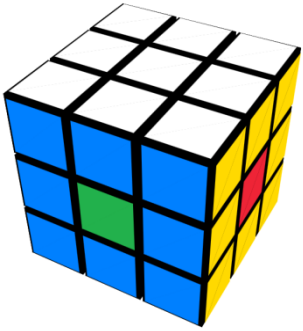


2Cube = AGAH'DHA^{2}G^{2}H'G'PB'P'G^{2}H



6Spot = HB'DG'AP'HB'

3Cube = H'G'H'A' D^2 P'DA $HP^2HP'G$ H'AHDA'



4Spot = Ω = $A^2P^2HB' D^2G^2HB'$

L'un des facteurs du SuperFlip4Spot ∏

SuperFlip = Φ = $D'H^2PG'$ .AH'PBA .HB'GB^2 .A'DP'BA' .H'P'HB'

SuperFlip4Spot =

$\prod = H^2B^2G\ A^2\ .H'BD^2\ PH'B'D.\ GA^2D\ HB'\ D'GHA'P'$

$\prod = \Phi\Omega = \Omega\Phi$

Le SuperFlip4Spot est un SuperLoin (longueur = 26) le seul qu'on connaît !

25 SOLUTION DU RUBIK'S CUBE

Un livre sur le Rubik's Cube sans algorithme de résolution n'est pas un livre sur le Rubik's Cube ! il est donc raisonnable de fournir un algorithme de résolution dans ce dernier chapitre.

Un algorithme de résolution est une sorte de recette cuisine qui permet de restaurer le Cube, càd une suite finie d'instructions qui permet de placer, pivoter , ranger ... les pièces.

À chaque étable de résolution on peut tenir le Cube comme on veut et on peut utiliser la conjugaison. En Cubologie les formules utiliser doivent provenir des rotations de base, des rotation standards.

Ainsi en Rubik's Cube les formules ne doivent contenir que {H,B,A,P,G,D} mais dans la pratique on fait ce qu'on veut pour vu que ça marche, par ex on peut utiliser les rotations tranches {h, d, a} ou rotations Cube ${}^{t}H$, ${}^{t}B$ ou rotations bloc H*, B* , etc .....

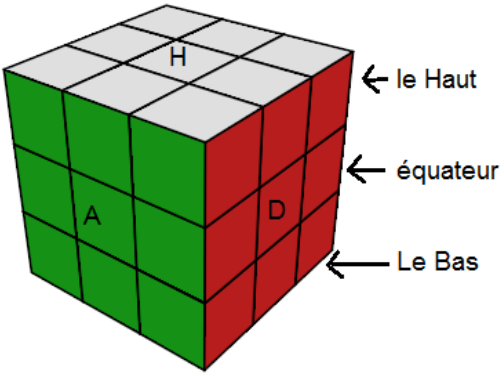
Par exemple, il est plus simple de pivoter les centres (H) et (A) avec la formule (non-standard)

$(H)^{+}(A)^{-}$ = Ha'h'a . H'a'ha

que la formule
$(H)^{+}(A)^{-}$ = AP' GD' HB' .A' .BH' DG' PA' .H

Résolution du Rubik's Cube :

L'algorithme [DH] Auteur: Morphocode
Année: 2011



Cette méthode se divise en 5 étapes, et chaque étape utilise 2 formules donc en tout 10 formules pour restaurer le Cube. La stratégie est très classique, étage par étage. On finit d'abord le Bas (1ère étage) puis l'équateur (2ère étage) puis le Haut (3ème étage)

- Finir le Bas: ranger les arêtes puis les sommets
- Finir l' équateur
- Finir le Haut: ranger les arêtes puis les sommets

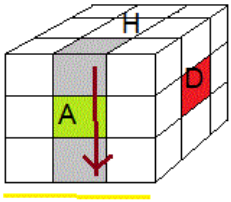
Pour fixer les idées on va prendre un Rubik's Cube standard avec:

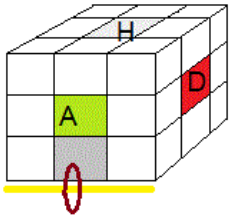
(H)aut = (b)lanc, (B)as = (j)aune, (A)vant = (v)ert, (P)ostérieur = (k)lein, (G)auche = (o)range, (D)roite = (r)ouge .

25.1 RANGER LES ARÊTES BAS

On va ranger (placer et orienter) les arêtes Bas c'est-à-dire on fait la Croix en Bas.

Trouve l'arête-Bas (jv) , puis place-la juste au dessus et ensuite on fait un A^2 pour descendre l'arête.
Si (jv) est mal orienté, on la renverse par la formule:
$(BA)^+ = BDB'.A$





$(HA) \rightarrow (BA) = A^2$ $(BA)^+ = BDB'.A$

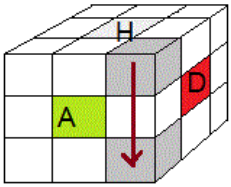
25.2 RANGER LES SOMMETS BAS

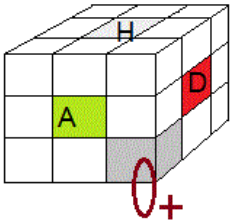
On va ranger (placer et orienter) les sommets Bas c'est-à-dire on va finir le Bas.

Trouve le sommet-Bas (jvr), puis place le juste au dessus

(voir fig), puis on le descend par la formule:
[DH] = DHD'H'

Si (jvr) est mal orienté on le pivote (2 fois si nécessaire) par la formule:
$(BAD)^{+} = [DH]^2$





(HDA)-→(BAD) = [DH] = DHD'H' $(BAD)^{+} = [DH]^2$

Remarque : Si un sommet se trouve dans un mauvais emplacement, on le déloge en y mettant n'importe quoi !! .

On fait la même chose pour les autres sommets Bas (sommets jaunes)

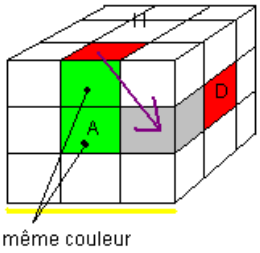
25.3 RANGER LES ARÊTES-EQUATEUR

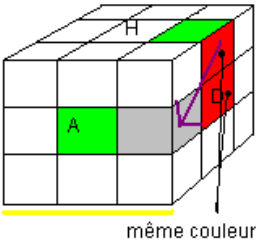
Trouvez une arête-équateur, c'est-à-dire une arête qui n'a pas de couleur Haut = blanc, puis positionne la bien

comme il le faut:
Suivant le cas on applique la formule correspondante:

* (HA) = (vr) , vert = A: (HA)→(AD) = [HD][H'A'] (on pourrait dire: [HD] = préparer et [H'A'] = placer)

* (HD) = (vr) , rouge = D: (HD)→(AD) = [H'A'][HD] (on pourrait dire: [H'A'] = préparer et [HD] = placer)





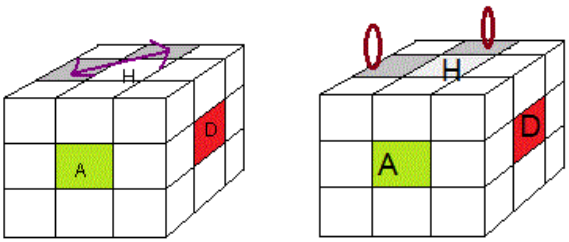
(HA)-→(AD) = [HD][H'A'] (HD)-→(AD) = [H'A'][HD]

Remarque : Si une arête se trouve dans un mauvais emplacement, on la déloge en y mettant n'importe quoi !! .

25.4 RANGER LES ARÊTES HAUT

On place les arêtes Haut grâce à la formule: A[DH]A'H
(HG)↔(HP) = A[DH]A'H

Les arêtes Haut sont bien placées maintenant, on va les orienter.
Renverser 2 arêtes adjacentes : $(HG)^+(HP)^+ = (A[DH]A'H)^2$



$(HG)\leftrightarrow(HP) = A[DH]A'H$ $(HG)^+(HP)^+ = (A[DH]A'H)^2$

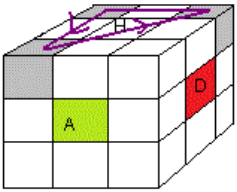
REMARQUE : Si on a 2 arêtes opposées à renverser, on applique simplement la même formule $(A[DH]A'H)^2$ et on revient au cas 2 arêtes adjacentes à renverser. Il ne faut surtout pas utiliser les conjugaisons car la formule n'est pas propre (ça détruira le Bas!!)

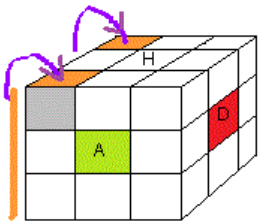
⚠ Quand on renverse les arêtes Haut, il est impossible de renverser une seule arête, on renverse toujours 2 arêtes. En effet la loi des flips dit que la somme des flips est un nombre pair. Si on renverse une seule arête le nombre de flip vaut 1 donc impair ce qui est impossible.

25.5 RANGER LES SOMMETS HAUT

On va placer les sommets Haut avec la formule:
$(HGP)\rightarrow(HAG)\rightarrow(HPD) = [DH]\ .G'[HD]G$

On oriente les sommets avec la formule: monter la couleur Gauche sur le Haut
$(HGP)^{-}(HAG)^{+} = [DH]^2 .G'[HD]^2G$





$(HGP) \rightarrow (HAG) \rightarrow (HPD) = [DH] .G'[HD]G$ $(HGP)^{-}(HAG)^{+} = [DH]^2 .G'[HD]^2G$

<u>Remarque</u> : Cette formule est propre, donc on peut utiliser la conjugaison sans prendre des précautions.

⛛ Quand on place des sommets Haut, il est impossible de permuter deux sommets. En effet la loi de parité dit que la signature des sommets doit être égale à la signature des arêtes sig(sommets) = sig(arêtes) . Or si on permute deux sommets la signature des sommets est impair sig(sommets) = impair tandis que la signature des arêtes est paire car toutes les arêtes sont bien placées, permutation identique id, sig(arêtes) = pair. donc c'est impossible

⛛ Quand on pivote les sommets Haut, il est impossible de pivoter un seul sommet 1/3 ou 2/3 de tour on pivote toujours 2 sommets ou 3 sommets. En effet la loi des twists dit que la somme des twists est un multiple de 3. Si on pivote un seul sommet 1/3 ou 2/3 de tour le nombre

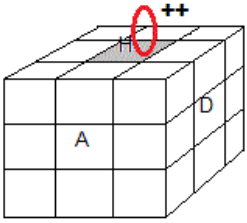
de twists vaut 1 ou 2 ce n'est pas un multiple de 3 donc c'est impossible.

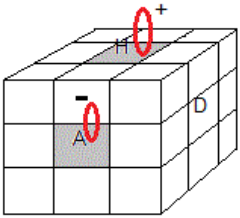
25.6 PIVOTER LES CENTRES

Voici deux formules supplémentaires pour pivoter les centres, si jamais vos centres sont orientés du genre: Hello Kitty Cube , Fisher Cube ...

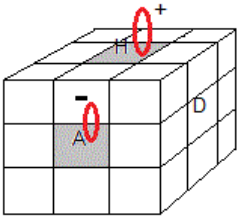
Pivoter le centre Haut à 180°:
$(H)^{++} = (HDG.H^2D'G')^2$
Pivoter le centre Haut à 90° et Gauche à -90°:
$(H)^{+}(A)^{-} = Ha'h'a\ .\ H'a'ha$
Ou encore : $(H)^{+}(A)^{-} = AP'\ GD'\ HB'\ .A'\ .BH'\ DG'\ PA'\ .H$

Remarque : certains auteurs notent: $A_s = AP'$ (A,P même direction) , $D_a = DG$ (D,G direction contraire)
$(H)^{++} = (HD_aH^2D'_a)^2$
$(H)^{+}(A)^{-} = A_sG_sH_s.\ A'\ .\ B_sD_sP_s\ .H$





$(H)^{++} = (HDG.H^2D'G')^2$ $(H)^{+}(A)^{-} = Ha'h'a.H'a'ha$



$(H)^{+}(A)^{-} = AP'\ GD'\ HB'\ .A'\ .BH'\ DG'\ PA'\ .H$

Et voilà, maintenant le Rubik's Cube n'a plus de secrets pour vous .....

26 LES FORMULES SUPPLÉMENTAIRES

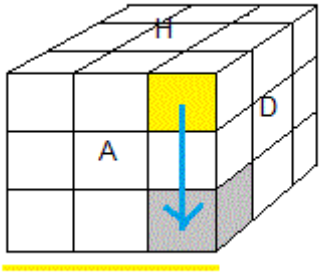
C'est la caverne d'Ali Baba !! vous trouverez ici les raccourcis, les formules de toute sorte pour s'en sortir ou aller plus vite ....

I. Les raccourcis

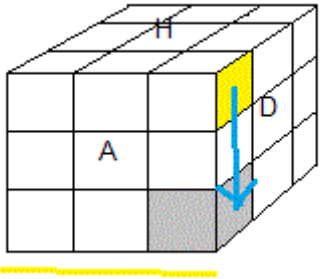
Vous avez réussi à restaurer le Cube avec ces 10 formules, mais vous voulez peut-être aller plus vite. Il existe des raccourcis! Il suffit d'apprendre par cœur et adapter à chaque situation.

Pour descendre le sommet (HDA)→(BAD)

Le sommet (HDA) ne peut avoir que 3 situations:
1. si la couleur du Bas (jaune) se trouve sur l'Avant on le descend directement par: [HD]
2. si la couleur du Bas (jaune) se trouve sur la Droite on utilise: [H'A']
3. si la couleur du Bas (jaune) se trouve sur le Haut on le pivoter:

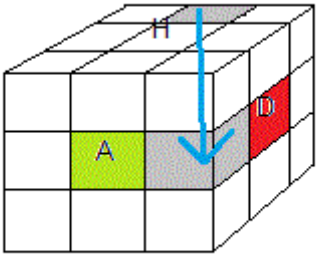


(HDA)→(BAD) = [HD]

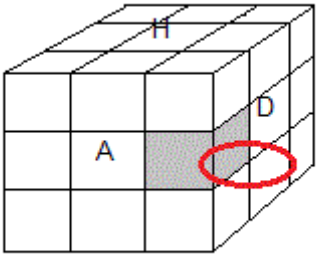


(HDA)→(BAD) = [H'A']

Placer: (HP)→(AD) = [D'A][HD]' = [D'A][DH] (découverte par moi, commutateur Y = [D'A] et Z = [HD])
Renverser l'arête (AD): $(AD)^{+} = (DH^2D'H)^2$ .A'H'A



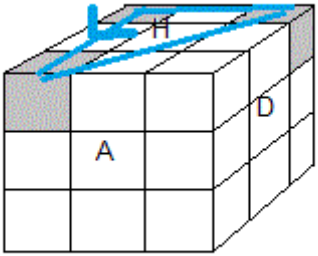
$(HP)\rightarrow(AD) = [D'A][DH]$



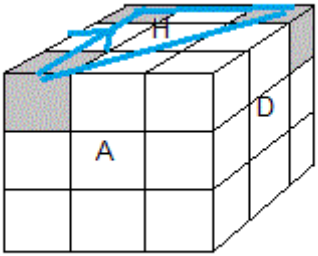
$(AD)^{+} = (DH^{2}D'H)^{2}\ .A'H'A$

II. <u>Permutations inverses</u>

Rotation inverse les 3 sommets



(HGP)→(HAG)→(HPD) = [HD].G'[DH]G



(HGP)←(HAG)←(HPD) = G'[HD]G.[DH]

III. <u>Permuter sommets et arêtes</u>

Glisser: (HAG)↔(HPD).(HA)↔(HD) =
A'HA'H'.D'BD'B'.D^2[A'D']A
Glisser: (HGP)↔(HPD).(HA)↔(HD) = [D'H^2]D'AD.
HD'H'D'.A'D^2H'
Glisser: (HGP)↔(HPD).(HA)↔(HD) = [PH]P'D .P^2H'
.[P'H']P'D'

Glisser: $(HGP)\leftrightarrow(HPD).(HA)\leftrightarrow(HD) = HD^2H'D^2B.P^2G^2HG^2B'.P^2$

IV. Formules pour les arêtes

On ne touche pas les sommets bien sûr

$(HG)\rightarrow(HD)\rightarrow(HP) = D^2.H'D'H'.(DH)^2.DH'D$ (gsps = gilsser sans perturber les sommets)

$(HA)\rightarrow(HP)\rightarrow(HD) = D^2.HAP'.D^2.PA'\ H.D^2$; glisser 3 arêtes

$(HA)^+(HD)^+ = AH^2A^2\ .B'\ [H'G'\ ]B\ .A^2H'\ A'\ H'$ (formule propre)

$(HA)^+(HD)^+ = (AHB'G^2H^2B^2D)\ H\ (D'B^2H^2G^2BH'A')\ H'$ (commutateur, formule propre)

$(HA)\leftrightarrow(HD).(BA)\leftrightarrow(BD) = B^2DG'\ BH'\ DHB'\ A^2GD'\ B'$

$(HA)^+(HP)^+ = AH'\ DA'\ H.DG'.P'\ HD'\ PH'.GD'$

$(HA)\leftrightarrow(HP).(AD)\leftrightarrow(PD) = (D^2H^2)^3$

V. Formules pour les sommets

$(HDA)\rightarrow(HPD)\rightarrow(HGP) = PG'PD^2\ .P'GPD^2\ .P^2$ (gspa = glisser sans perturber les arêtes)

$(HGP)\rightarrow(HAG)\rightarrow(HDA) = AD'AG^2\ .A'DAG^2\ .A^2$ (gspa)

$(HDA)\rightarrow(HPD)\rightarrow(HAG) = HGH'.D'.HG'\ H'.D$ (ne perturbe pas les arêtes!!!)

$(HGP)\rightarrow(HAG)\rightarrow(HPD) = GA'GP^2 .G'AGP^2 .G^2$;glisser 3 sommets

$(HDA)\leftrightarrow(HAG) = PH' A' HP' H' AH^2$

$(HDA)\leftrightarrow(HPD) = (D^2H)^2(D^2H^2)^2 .A^2H' A^2HA^2H'$ (perturber les arêtes)

$(HDA)^+(HPD)^+(HPG)^+ = DHD'H .DH^2D'H^2$ (perturber arêtes)

$(HGP)\rightarrow(HDA)\rightarrow(HPD) = D^2 .P^2DAD'. P^2DA' D$; glisser 3 sommets

$(HAG)^-(HDA)^+ = D'BDABA'. H'.AB'A'D'B'D.H$

$(HAG)^- (HGP)^+ = DHD'H .DH^2D'H^2 .D'H'DH' .D'H^2DH^2$

VI. <u>Quatre formules indépendantes</u>

$(HG)\rightarrow(HD)\rightarrow(HP) = P^2H'G'D.P^2GD'H'.P^2$ (longueur = 9f)

$(HA)^+(HD)^+ = AH^2A^2 .B' [H' G']B. A^2H' A' H'$ (longueur = 13f)

$(HDA)\rightarrow(HPD)\rightarrow(HGP) = D^2 .P^2DAD'. P^2DA' D$ (longueur = 9f)

$(HAG)^-(HDA)^+ = HAB'A^2H .G^2H'G^2. AH'A^2BA^2$ (longueur = 13f)

Ces formules sont indépendantes, avec H , elles permettent de restaurer le Cube dans l'ordre comme on veut: arêtes puis sommets (ou l'inverse)
Si l'état du Cube est localement impair (sig(u) = sig(v) = -

1) on fait un H avant d'appliquer l'algorithme.
Pour les arêtes: Placer puis orienter (ou l'inverse)
Pour les sommets: Placer puis orienter (ou l'inverse)

Ces formules sont trouvées par Cube Explorer (Cube.exe), elles sont minimales mais n'ont aucune structure !! on ne comprend rien ce que fait la formule !!!

VII. Les formules dans <H,D>

Quand on mélange le Cube uniquement par H,D et que la résolution doit aussi utiliser ces deux rotations, on doit avoir les formules seulement en H,D. (les siamois)

Déplacer
$(HG)\rightarrow(HD)\rightarrow(HP) = D^2H'\ D'\ H'.(DH)^2.DH'\ D$;glisser

Pivoter
$(HGP)^+(HAG)^- = DHD'H\ .DH^2D'H^2.D'H'DH'D'.H^2DH^2$
$(HPD)^+(HDA)^- = (DH')^3(D'H)^3$; perturber les arêtes
$(HDA)^+(HPD)^- = (D'H[DH'])^3\ .H'(D'H[DH'])^{-3}H$
$(HAG)^+(HGP)^+(HPD)^+ = (\ [H'D]^2\ .H'[DH']^2H\ )^2$
$(HDA)^+(HPD)^+(HGP)^+ = DHD'H\ .DH^2D'H^2$

Pivoter les centres
$(H)^{2+} = (DHD'\ H)^5$
$(H)^+(D)^- = D'\ K\ .(H'\ K)^2\ .H'\ D$ avec $K = (D'\ H'\ )^2D(HD)^2$; pas évident à trouver !

De même on peut imposer de mélanger le Cube uniquement par les rotations H,D,A et que la résolution utilise aussi uniquement ces rotations. On doit donc avoir les formules comportant uniquement H,D,A (pas évident !)

27 CODAGES DES PIÈCES

Numérotation des pièces

Arêtes : $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}$

Sommets : $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$

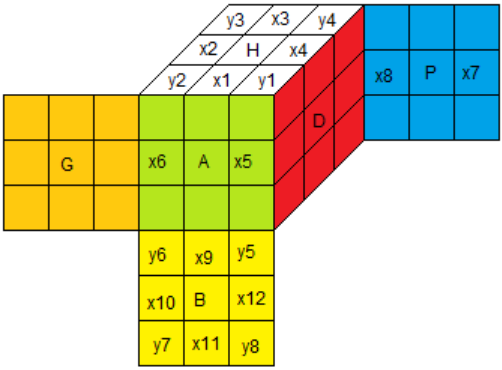


Diagramme des numérotations des pièces

Marquages des facettes

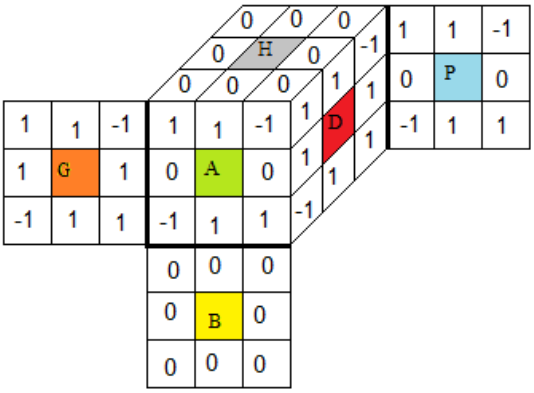


Diagramme des marquages

Numérotation des autocollants

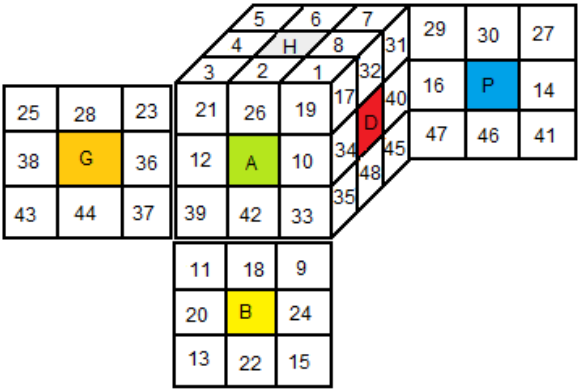


Diagramme des autocollants numérotés

TABLE DES MATIÈRES

Biographie

* Cube Explorer (Herbert Kociemba) : On donne un état, il trouve une formule correspondant en face-métrique ou quart-métrique.

http://kociemba.org/cube.htm

* Voici les javascripts pour calculer l'ordre maximal et l'ordre d'un élément.

https://fan2cube.fr/javascript/ordre_maxi.html

https://fan2cube.fr/javascript/ordre_calcul.html

* GAP, est un programme qui permet de calculer, l'ordre d'un groupe de permutations, ...

https://www.gap-system.org/Releases/index.html

* Les quiz pour tester vos connaissances

https://fan2cube.fr/certificat/mc1.html

* Un simulateur des cubes

http:/pMetro.su/pCubes.zip

* Rubik résolution

https://fan2cube.fr/softs/rubiks-solver-master.zip

* Rubik animation

https://fan2cube.fr/softs/rubik_animation.zip

* Virtualcube

https://fan2cube.fr/softs/virtualcubejs2017.zip

Du même auteur

¤*1 La conjecture de Fermat*

C'est un livre qui démontre la conjecture de Fermat, (appelé souvent "le dernier théorème de Fermat") en s'appuyant sur deux théorèmes: le théorème de Ribet et le théorème de Wiles. Un document rare et exceptionnel.

¤*2 La Relativité Générale*

Tout sur la Relativité Générale et on trouve une démonstration de l'équation tensorielle d'Einstein à partir du principe moindre action, ce qui est très rare.

¤*3 Le Groupe du Rubik's Cube (Tome I, II)*

Le Rubik's Cube possède un groupe très riche en propriétés et si la partie mathématique du puzzle vous intéresse alors ce livre est pour vous.

¤*4 La Relativité Restreinte*

La Relativité Restreinte est une théorie physique proposée par Einstein pour remplacer la mécanique newtonienne quand la vitesse des objets est proche à celle de la lumière c.

¤*5 Les nombres transcendants*

Les nombres transcendants sont très mystérieux, ils sont partout, beaucoup plus nombreux que les nombres algébriques et pour tant on connaît très peu de ces nombres, le premier est e, puis π, cos(1) , ...

¤*6 La Cubologie (Tome I, II)*

Pour comprendre les propriétés des twists il faut passer par les mathématiques, à chaque twist on associe un groupe et ce sont des propriétés de ce groupe qui expliquent les propriétés du twist.

¤*7 La physique quantique (Tome I, II)*

Si vous voulez savoir ce que c'est la physique quantique , ce livre est pour vous.