Rubik's cube et la théorie des groupes

Anastasiia Chernetcova, supervisé par Yves Aubry

Mars 2022



Introduction

- \bullet Le cube se compose de 3^3 petits cubes;
- 2 7 sont fixes:
 - le cube central;
 - le cube au centre des tranches (3).et 20 mobiles :
 - Les coins, au nombre de 8 (1);
 - 2 Les arêtes, au nombre de 12 (2).

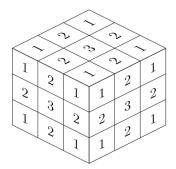


Figure - Les parties fixes et mobiles du cube

Introduction

But du jeu = résoudre le Rubik's cube, ie le ramener dans son état d'origine.

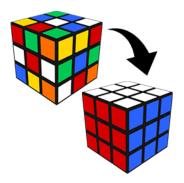


Figure - Résoudre le Rubik's cube

Notations et vocabulaire

- Tranche du Rubik's cube = partie tournante composée de 9 pièces;
- On notera les faces U, F, L, R, B, D.
- U, F, L, R, B, D seront aussi les rotations dans le sens des aiguilles d'une montre des mêmes faces. On notera R⁻¹ la rotation dans le sens contraire des aiguilles d'une montre.

Groupe du Rubik's cube

On notera les coins comme indiqué dans la figure 3 et les arêtes comme indiqué dans 4.



Figure – Numérotation des coins



Figure – Numérotation des arêtes

Groupe du Rubik's cube

- **(** (*Rub*, ∘) contient toutes les transformations du Rubik's cube engendrées par les rotations des 6 tranches.
- **3** $Rub = \text{groupe de Rubik's cube } légal, <math>G \supset Rub = \text{groupe du Rubik's cube } illégal \text{ ou élargi.}$

Groupe du Rubik's cube

- **9** Posons G_C le groupe d'action sur les coins et G_A le groupe d'action sur les arêtes. $G \simeq G_C \times G_A$.
- ② $ord(G_C) = 8! \times 3^8$.
- $ord(G_A) = 12! \times 2^{12}.$
- $ord(G) = ord(G_C) \times ord(G_A) = 8! \times 3^8 \times 12! \times 2^{12}$.

Théorème 0.1

Rub est un sous-groupe de G d'indice 12.

Corollaire 1

$$| Rub | = \frac{1}{12} \times 8! \times 3^8 \times 12! \times 2^{12} \simeq 43 \times 10^{18}.$$



Construction du groupe de Rubik's cube

Objectif : montrer que $G \simeq ((\mathbb{Z}/3\mathbb{Z})^8 \rtimes \mathfrak{S}_8) \times ((\mathbb{Z}/2\mathbb{Z})^{12} \rtimes \mathfrak{S}_{12}).$

$$\forall g \in G, g = (\pi_C(g), \pi_A(g)).$$

- **1** $\pi_C: G \to G_C$ est la projection canonique de G sur G_C qui laisse fixe A;
- ② $\pi_A: G \to G_A$ est la projection canonique de G sur G_A qui laisse fixe C.



Figure – Les 3 facettes d'un coin

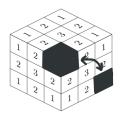


Figure – Les permutations des coins

Si l'on ne regarde que les positions des coins, il existera un morphisme

$$\sigma_C: \begin{array}{ccc} {\cal G}_C & \longrightarrow & {\mathfrak S}_C \simeq {\mathfrak S}_8 \\ g & \longmapsto \sigma_C(g) \end{array}.$$

- σ_C surjectif;
- $Ker(\sigma_C) = Rot_C$, le groupe qui contient les rotations des coins.



- $\rho_C: G_C \to \mathbb{Z}/3\mathbb{Z}^8$ associe à $g \in G_C$ le pivotement des coins.
- $\rho_C(g) = (n_1, \ldots, n_8).$
- Si g agit sur un coin j, alors g orientera le coin j de n_j tiers de tour dans le sens direct.
- Groupe cyclique d'ordre 3, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$;
- $Rot_C \simeq (\mathbb{Z}/3\mathbb{Z})^C \simeq (\mathbb{Z}/3\mathbb{Z})^8$.

F	(2,0,0,1,1,0,0,2)
D	(0,0,0,0,0,0,0,0)
F∘U	(2,0,0,1,1,0,0,2)

Table – Les orientations des coins induites par les rotations F, D, $F \circ U$

• $g \in G_C$ se décompose en le produit $\rho_C(g)\sigma_C(g)$ et cette écriture est unique.

Remarque 1

$$hg = \rho_C(h)\sigma_C(h)\rho_C(g)\sigma_C(g) = \underbrace{\rho_C(h)\sigma_C(h)\rho_C(g)\sigma_C(h)^{-1}}_{\rho_C(hg)}\underbrace{\sigma_C(h)\sigma_C(g)}_{\sigma_C(hg)}.$$

- Relation caractéristique d'un produit semi-direct interne.
- $G_C \simeq \mathbb{Z}/3\mathbb{Z}^8 \rtimes \mathfrak{S}_8$.

- $\forall \rho \in Rot_C, \rho = (n_x)_{x \in C} \in (\mathbb{Z}/3\mathbb{Z})^C$, où chaque coin x subit une rotation de n_x tiers de tour.
- Rotation totale de $g: rt_C(g) := \sum_{x \in C} n_x \in \mathbb{Z}/3\mathbb{Z}$.

Lemme 1

 $rt_C: (G_C, \circ) \to (\mathbb{Z}/3\mathbb{Z}, +)$ est un morphisme de groupes.



Remarque 2

Pour tout $g, h \in G_C$ tels que $\rho_C(g) = (n_x)_{x \in C}$ et $\rho_C(h) = (n_x')_{x \in C}$, si l'on note $\rho_C(gh) = (n_x'')_{x \in C}$ on a, pour tout $x \in C$:

$$n_x''=n_x+n_{\sigma^{-1}(g)(x)}'.$$

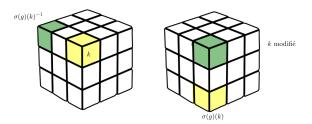


Figure - Schéma explicatif

Démonstration du lemme.

• Soient $g, h \in G_C$, où $g = \rho_C(g)\sigma_C(g)$ et $h = \rho_C(h)\sigma_C(h)$. Notons $gh = \rho_C(gh)\sigma_C(gh)$.

•

$$gh = \rho_{C}(g)\sigma_{C}(g)\rho_{C}(h)\sigma_{C}(h)$$

$$= \underbrace{\rho_{C}(g)\sigma_{C}(g)\rho_{C}(h)\sigma_{C}(g)^{-1}}_{\rho_{C}(gh)}\underbrace{\sigma_{C}(g)\sigma_{C}(h)}_{\sigma_{C}(gh)}.$$

•
$$\rho_C(gh) = (n_x'')_{x \in C} = n_x + n_{\sigma_C(g)(x)^{-1}}'$$
.

•
$$rt_C(gh) = \sum_{x \in C} (n_x + n'_{\sigma_C(g)(x)^{-1}}) = \sum_{x \in C} (n_x + n'_x).$$





Figure - Les permutations des arêtes

Si l'on ne regarde que les positions des arêtes, il existera un morphisme

$$\sigma_A: egin{array}{ccc} G_A & \longrightarrow & \mathfrak{S}_A \simeq \mathfrak{S}_{12} \\ g & \longmapsto \sigma_A(g) & \end{array}$$

- σ_A surjectif;
- $Ker(\sigma_A) = Rot_A$, le groupe qui contient les rotations des arêtes.

- $\rho_A: G_A \to \mathbb{Z}/2\mathbb{Z}^{12}$ associe à $g \in G_A$ le pivotement des arêtes.
- $\rho_A(g) = (m_1, \ldots, m_{12}).$
- Si g agit sur la j^e arête, alors g orientera cette arête de m_j demies de tour.
- Groupe cyclique d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$;
- $Rot_A \simeq (\mathbb{Z}/2\mathbb{Z})^A \simeq (\mathbb{Z}/2\mathbb{Z})^{12}$.

F	(1,0,0,0,0,0,0,0,1,0,0,0)
D	(0,0,0,0,0,0,0,0,0,1,0,1)
F o U	(1,0,1,0,1,0,0,0,1,0,0,0)

Table – Les pivotements d'arêtes induites par les mouvements élementaires

- $g \in G_A$ se décompose en le produit $\rho_A(g)\sigma_A(g)$ et cette écriture est unique.
- $G \simeq Rot_A \rtimes \mathfrak{S}_A$.
- $\forall \rho \in Rot_A, \rho = (m_y)_{y \in A} \in (\mathbb{Z}/2\mathbb{Z})^A$, où chaque arête y subit une rotation de m_y demis de tour.
- Rotation totale de $g: rt_A(g) := \sum_{y \in A} m_y \in \mathbb{Z}/2\mathbb{Z}$.

Lemme 2

 $rt_A: (G_A, \circ) \to (\mathbb{Z}/2\mathbb{Z}, +)$ est un morphisme de groupes.

Théorème fondamental du Rubik's cube

Soit $g \in G$. On écrit

 $g = \rho_C \sigma_C \rho_A \sigma_A, \rho_C \in Rot_C, \rho_A \in Rot_A, \sigma_C \in \mathfrak{S}_C, \sigma_A \in \mathfrak{S}_A.$

Soit $E: g \to \{\pm 1\}$, $E(g) = \varepsilon(\sigma_A(g))\varepsilon(\sigma_C(g))$.

On a le morphisme suivant

$$rt: \begin{array}{ccc} G & \longrightarrow & \{\pm 1\} \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ g & \longmapsto (E(g), rt_C \circ \pi_C(g), rt_A \circ \pi_A(g)) \end{array}$$

[G: Ker(rt)] = 12.

Théorème 0.2

Rub = Ker(rt), ie

$$g \in G \iff \begin{cases} E(g) = 1\\ \sum_{x \in C} n_x = 0 \text{ [3]}\\ \sum_{y \in A} m_y = 0 \text{ [2]} \end{cases}$$



Montrons l'inclusion $Rub \subset Ker(rt)$.

- Un mouvement élementaire induit un 4-cycle sur les coins et un 4-cycle sur les arêtes. Ce sont des cycles à support disjoint. Donc E(g)=1 pour tout g produit de mouvements élementaires.
- F= ensemble des facettes des arêtes. on a |F|=24. Un mouvement élementaire induit deux 4-cycles sur les facettes des arêtes. Comme c'est un produit de 4-cycles, il est de signature paire.
- On prend deux faces privilégiées U et D par exemple. La rotation U (ou D) ne pivote pas les coins. La rotation F (par exemple) pivote les deux coins $x_{U,F,R}$ et $x_{U,F,L}$ de 1 et de 2 tiers de tour. Leur somme est nulle dans $\mathbb{Z}/3\mathbb{Z}$.

Quelques rappels

• Le groupe G des mouvements du Rubik's cube (y compris illégaux) est isomorphe à

$$((\mathbb{Z}/3\mathbb{Z})^8 \rtimes \mathfrak{S}_8) \times ((\mathbb{Z}/2\mathbb{Z})^{12} \rtimes \mathfrak{S}_{12}).$$

• Un élément $g \in G$ se décompose naturellement en $g = \sigma_A(g)\rho_A(g)\sigma_C(g)\rho_A(g)$.

On a le morphisme suivant

$$rt: \begin{array}{ccc} G & \longrightarrow & \{\pm 1\} \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ g & \longmapsto (E(g), rt_C \circ \pi_C(g), rt_A \circ \pi_A(g)) \end{array}$$

Le sous-groupe Rub de G contient toutes les opérations "légales".



Si g est un mouvement légal, alors g vérifie le théorème suivant :

Théorème 0.3

$$g \in Rub \iff \begin{cases} E(g) = \varepsilon(\sigma_A(g))\varepsilon(\sigma_C(g)) = 1\\ \sum_{x \in C} n_x = 0 \ [3]\\ \sum_{y \in A} m_y = 0 \ [2] \end{cases}$$

On a montré que $Rub \subset Ker(rt)$.

Aujourd'hui, on montrera que $Ker(rt) \subset Rub$. On présentera aussi quelques sous-groupes du groupe Rub, à savoir

- Le groupe des quaternions;
- 2 Le groupe "carré" (square group).

Algorithme de résolution du Rubik's cube

La démonstration de $Ker(rt) \subset Rub$ est plutôt constructive. On doit introduire l'algorithme de résolution du Rubik's cube. Cet algorithme consiste à :

- mettre les arêtes à leur place;
- les retourner 2 à 2 afin de les orienter correctement;
- appliquer les 2 étapes précédentes aux coins sans toucher aux arêtes.

Notations

- $y_{\alpha,\beta}$ l'arête commune aux faces α,β ;
- $x_{\alpha,\beta,\gamma}$ le coin commun aux faces α,β,γ .

On notera $g = \sigma_C(g)\rho_C(g)\sigma_A(g)\rho_A(g) = \sigma_C\rho_C\sigma_A\rho_A$, $\sigma_C \in \mathfrak{S}_8, \sigma_A \in \mathfrak{S}_{12}, \rho_C \in \mathbb{Z}/8\mathbb{Z}^8, \rho_A \in \mathbb{Z}/2\mathbb{Z}^{12}$.



Pivotement (rotation) des arêtes

Cas spécial :
$$\sigma_A = id$$
, $\sigma_C = id$, $\rho_C = (0, ..., 0)$.

$$h = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$$

pivote $y_{U,F}$ et $y_{U,R}$.



Figure – Le mouvement qui pivote deux arêtes

Pour tout couple d'arêtes (y_1, y_2) , il existe $g \in Rub$ qui envoie y_1 sur $y_{U,F}$ et y_2 sur $y_{U,R}$. Il s'en suit que ghg^{-1} réoriente deux arêtes y_1 et y_2 quelconques.

Pivotement (rotation) des arêtes

- Ker $(\sigma_A \circ \pi_A)$ contient $g \in Rub$ qui laissent invariantes les positions des arêtes, mais qui peuvent éventuellement modifier leur orientation.
- $Rot_A^0 \subset Rot_A =$ les éléments de rotation totale nulle.

Lemme 3

 $\pi_A : \mathsf{Ker}(\sigma_A \circ \pi_A) \cap Rub \to Rot_A^0$ est surjective.

Pivotement (rotation) d'arêtes

Démonstration.

- $\forall y_1, y_2 \in A$, il existe $g \in Rub$ tel que ghg^{-1} retourne y_1 et y_2 sans toucher aux autres arêtes.
- $Rub \cap Ker(\sigma_A \circ \pi_A)$ contient les rotations d'arêtes légales.
- $\pi_A(Rub \cap \text{Ker}(\sigma_A \circ \pi_A))$ contient les retournements d'arêtes quelconques. Les élements de cet ensemble engendrement Rot_A^0 , car tout $r \in Rot_A^0$ est composé d'un nombre **pair** de retournements d'arêtes (théorème fondamental).



Pivotement de coins

$$\sigma_A = id, \sigma_C = id, \rho_A = (0, \dots, 0).$$

$$\gamma = (R^{-1}D^2RB^{-1}U^2B)^2$$

tourne $x_{U,F,R}$ d'un tiers de tour et $x_{B,D,L}$ de deux tiers de tour.

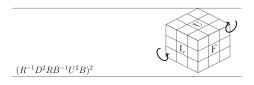


Figure – Le mouvement pivotant $x_{U,F,R}$ et $x_{B,D,L}$

Pour tout couple x_1, x_2 de coins, il existe $g \in Rub$ qui envoie x_1 sur $x_{U,F,R}$ et x_2 sur $x_{B,D,L}$. Il s'en suit que $g\gamma g^{-1}$ réoriente x_1 et x_2 sans déranger les autres coins.

Pivotement de coins

• $Rot_C^0 \subset Rot_C = les$ mouvements de rotation totale nulle.

Lemme 4

 $\pi_C : Rub \cap Ker(\sigma_C \circ \pi_C) \to Rot_C^0$ est surjective.

Démonstration.

La démonstration est identique que pour le pivotement des arêtes.



Permutation des arêtes

Le mouvement

$$U^{-1}FULU^{-1}L^{-1}F^{-1} (1)$$

permute deux arêtes de la face U.

- Par conjugaison de 1, on peut transposer deux arêtes de A.
- Les transpositions engendrent \mathfrak{S}_A . Cela prouve qu'il existe un élement de Rub qui envoie les arêtes à leur emplacements respectifs.

Permutation des coins

- Une fois les arêtes mises en place, on sait que la permutation opérant sur les coins doit être paire.
- Le groupe alterné \mathfrak{A}_C est engendré par les 3-cycles.
- On montre qu'il existe un 3-cycle agissant sur un triplet de coins quelconque.

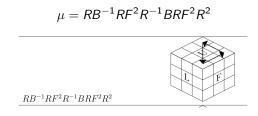


Figure – Le mouvement μ

Ce mouvement agit par 3-cycle sur les coins $x_{U,F,L}, x_{U,F,R}, x_{U,B,R}$. Pour tout $x \in C$, il existe $g \in Rub$ qui envoie x sur la position d'un de ces 3 coins. On peut ainsi construire un 3-cycle sur n'importe quel triplet de coins.

Résolution du Rubik's cube

- c₀ est une configuration de Ker(rt).
- On applique à c_0 une suite de mouvements g exposés ci-dessus.
- On aboutit à $c_0 \circ g = 1_{Rub}$.
- $g^{-1} = c_0$, donc $c_0 \in Rub$.
- Ainsi $Ker(rt) \subset Rub$. A ce stade, on a prouvé que Ker(rt) = Rub.

Quelques sous-groupes remarquables du groupe du Rubik's cube

Le groupe des quaternions

Le groupe des quaternions $\mathcal Q$ (muni de la multiplication) est défini ainsi :

$$Q = \{i, j, k \mid i^2 = j^2 = k^2 = ijk = -1\}.$$

Remarque 3

- \bullet i, j, k sont d'ordre 4 dans Q.
- $i^{-1} = -i, j^{-1} = -j, k^{-1} = -k.$

Le groupe des quaternions

On considère les manoeuvres suivantes :

- 0 1 := id;
- ② −1 := m_{435} qui pivote les arêtes y_{UF} , y_{UL} , y_{UB} , y_{UR} d'une demie de tour dans le sens des aiguilles d'une montre;
- i = m₇₀₆ qui transpose y_{UR} et y_{UF} en pivotant y_{UR} d'une demie de tour et qui transpose y_{UL} et y_{UB} en pivotant y_{UL} d'une demie de tour;
- j = m₇₀₇ qui transpose y_{UL} et y_{UF} en pivotant y_{UL} d'une demie de tour et qui transpose y_{UB} et y_{UR} en pivotant y_{UB} d'une demie de tour;
- **9** $k = m_{710}$ qui transpose y_{UF} et y_{UB} en pivotant y_{UF} d'une demie de tour et qui transpose y_{UL} et y_{UR} en pivotant y_{UL} d'une demie de tour.

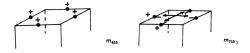


Figure – Les mouvements m_{435} et m_{710}

Le groupe des quaternions

On note $\mathcal R$ le groupe engendré par

 $-1=m_{435}, i=m_{706}, j=m_{707}, k=m_{710}.$ On a que (\mathcal{R},\circ) est un groupe dont les éléments vérifient les propriétés suivantes :

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

$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$
 (3)

On a un isomorphisme de groupes $\varphi: \mathcal{R} \to \mathcal{Q}$.

Démonstration.

On peut vérifier par un calcul fastidieux que les éléments de \mathcal{R} vérifient les propriétés du groupe de quaternions.



Propriétés du groupe des quaternions

Montrons que $\mathcal Q$ est d'ordre 8 dont les sous-groupes sont cycliques et distingués dans $\mathcal Q$.

- **1** $Q = \{1, -1, i, -i, j, -j, k, -k\}$, donc |Q| = 8.
- ② Q non commutatif, car ij = -ji. Le centre Z(Q) vaut $\{1, -1\}$.
- Les sous-groupes de Q différents de {1} et de Q sont d'ordre 2 ou 4 par le théorème de Lagrange.
 - $\langle -1 \rangle$ est le seul sous-groupe d'ordre 2. S'il existait un sous-groupe d'ordre 2 contenant i (ou j, ou k), alors il contiendrait aussi 1 et -i, donc 3 éléments (c'est absurde).
 - 2 Les seuls sous-groupes d'ordre 4 sont $\langle i \rangle, \langle j \rangle, \langle k \rangle$. S'il existait un sous-groupe d'ordre 4 contenant i et j par exemple, alors il contiendrait aussi -i et -j ainsi que 1, donc 5 éléments (absurde).

Donc tous les sous-groupes de $\mathcal Q$ sont cycliques.



Propriétés du groupe des quaternions

Proposition 1

Tous les sous-groupes de $\mathcal Q$ sont distingués dans $\mathcal Q$.

Démonstration.

- **1** Le centre Z(Q), $\langle -1 \rangle$, est distingué dans Q (abélien).
- 2 Montrons que $\langle i \rangle$ est distingué. On a

$$jij^{-1} = ji(-j) = -jij = ijj = i(-1) = -i,$$

 $kik^{-1} = ki(-k) = k(-ik) = kki = -i.$

Donc $\langle i \rangle$ est stable par conjugaison, donc distingué.

Remarque 4

On peut définir $\mathcal Q$ avec des matrices 2×2 à coefficients dans $\mathbb C$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

Le groupe carré (square group)

On pose
$$S = \langle U^2, F^2, L^2, R^2, D^2, B^2 \rangle$$
.

Théorème 0.4

Le groupe carré S est d'ordre 2¹³3⁴.

Démonstration.

S agit sur les arêtes et les coins indépendamment.

On note φ_A l'action du groupe S sur l'ensemble des arêtes. Elle admet trois orbites :

$$Orb(y_{UF}) = \{y_{UF}, y_{UB}, y_{DB}, y_{DF}\}$$

$$(4)$$

$$Orb(y_{UL}) = \{y_{UL}, y_{UR}, y_{DR}, y_{DL}\}$$

$$(5)$$

$$Orb(y_{FL}) = \{y_{FL}, y_{FR}, y_{BR}, y_{BL}\}$$
(6)

On fait la démonstration pour l'orbite 4



Le groupe carré

Démonstration.

• Montrons que y_{UF} , y_{UB} , y_{DB} , y_{DF} sont bien dans $Orb(y_{UF})$. On applique les mouvements suivants :

$$y_{UF} \xrightarrow{U^2} y_{UB}$$

$$y_{UF} \xrightarrow{F^2} y_{DF}$$

$$y_{UF} \xrightarrow{U^2B^2} y_{DB}.$$

- Montrons qu'aucune autre arête n'est dans Orb(yUF). En effet,
 - Le mouvement U^2 échange l'arête y_{UF} et y_{UB} ;
 - 2 Le mouvement F^2 échange y_{UF} et y_{DF} ;
 - **3** Le mouvement B^2 échange y_{UB} et y_{DB} ;
 - **3** Le mouvement D^2 échange y_{DF} et y_{DB} ;
 - **3** Les mouvements L^2 et R^2 laissent les 4 arêtes de cette orbite en place.



Le groupe carré

On note φ_C l'action de S sur les coins. Alors

$$Orb(x_{UFL}) = \{x_{UFL}, x_{UBR}, x_{DFR}, x_{DBL}\}$$
(7)

$$Orb(x_{UFR}) = \{x_{UFR}, x_{ULB}, x_{DRB}, x_{DLF}\}.$$
 (8)

- On peut placer les arêtes de (4!)³ façons.
- s ∈ S induit une transposition sur une paire d'arêtes d'une orbite donnée.
- Condition 1 du théorème fondamental \implies la permutation des coins ainsi que la permutation des arêtes doit être paire. Il reste donc $\frac{(4!)^3}{2} = 2^8 3^3$ emplacements possibles pour les arêtes.
- Par le théorème fondamental, la rotation totale des coins doit être nulle. Une fois que l'on a placé 4 coins, il reste 4 positions seulement pour les coins restants.

$$|S| = \frac{(4!)^3}{2} \cdot 4!4 = 2^8 \cdot 3^3 \cdot 2^5 \cdot 3 = 2^{13} \cdot 3^4.$$



What I learned in school



What's on the exam



What I know



Figure -