Méthodes combinatoires, problèmes de dénombrement

[Gou p357]

[De Biasi ch1]

190

I) Un peu de théorie des ensembles

1) Définitions

Def 1 Union, intersection

Soit $\mathcal{U}$ un ensemble, A et B deux parties de $\mathcal{U}$

on définit :

1) $A \cap B = \{x \in \mathcal{U}, x \in A \text{ et } x \in B\}$

2) $A \cup B = \{x \in \mathcal{U}, x \in A \text{ ou } x \in B\}$.

Si I est un ensemble, quelconque, et $(A_i)_{i \in I}$ une famille de parties de $\mathcal{U}$, on définit :

$$\bigcup_{i \in I} A_i = \{x \in \mathcal{U}, \exists i \in I, x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x \in \mathcal{U}, \forall i \in I, x \in A_i\}$$

Def 2 On dit que $\mathcal{U}$ est fini, ou de cardinal fini $m \in \mathbb{N}$ si :

$\mathcal{U} = \emptyset$ (et $m = 0$)

ou bien

si il existe une bijection $\varphi : \mathcal{U} \to [\![1, m]\!]$

not° : Card $\mathcal{U}$, $\#\mathcal{U} = m$.

Ex 3 $\mathcal{U} = \{0, 1, \dots, 4\} \to \{2, 4, 6, 8, 10\}$.

mais $\mathbb{R}$ ou $\bigcup_{m \in \mathbb{N}} \{-2m, 2m\}$ ne sont pas finis

2) Dénombrement d'ensembles

Prop 4 Soit $(E_i)_{i \in [\![1,m]\!]}$ m ensembles finis

$$\left| \bigcup_{1 \le i \le m} E_i \right| = \sum_{i=1}^{m} |E_i| - \sum_{1 \le i < j \le m} |E_i \cap E_j| + \sum_{1 \le i < j < k \le m} |E_i \cap E_j \cap E_k|$$

$$\dots + (-1)^m \left| \bigcap_{1 \le i \le m} E_i \right|$$

Ex 5 Cas $E_i \cap E_j = \emptyset$, $\forall i, j$, $\left| \bigcup_{1 \le i \le m} E_i \right| = \sum_{i=1}^{m} |E_i|$

Def 6 Soient A, B deux ensembles, $A \times B = \{(x, y), x \in A, y \in B\}$

Thm 7 $|A \times B| = |A| |B|$

Def 8 Soient $(A_i)_{1 \le i \le p}$ p ensembles finis

$(x_1, \dots, x_p)$ est une p-liste/uplet où $\forall k \in [\![1, p]\!]$, $a_k \in A_k$.

L'ensemble de ces p-liste est noté $A_1 \times \dots \times A_p$

Thm 9 $|A_1 \times \dots \times A_p| = \prod_{1 \le k \le p} |A_k|$

Appli 10 on compte p^m applications d'un m-ens dans un p-ens.

II) Combinatoire : un peu de probabilités

1) Arrangements, permutations, tirages

Soient $p, m \in \mathbb{N}$, $1 \le p \le m$ et E un m-ensemble.

Def 11 On appelle un p-arrangement de E un p-uplet $(e_1, \dots, e_p)$ où $\forall i \in [\![1, p]\!]$, $e_i \in E$ et $e_i \neq e_j$ $\forall i \neq j$

Rem 12 Vision via app° injective $\varphi : [\![1, p]\!] \to E$.

Notation p-arrangement : $\mathcal{A}_p$.

$\mathcal{A}_p$ s'identifie aux injections de $[\![1, p]\!]$ dans E

Thm 13 $|\mathcal{A}_p| = A_m^p := \frac{m!}{(m-p)!}$

Ex 14 prendre 2 crayons de couleurs d'une boîte de coloriage de 50 crayons : 2450 possibilités

Def 15 Si $p = m$ on parle de permutations

Ex 16 : Nombres de permutations d'un m-ensemble : $m!$

G_m : permutations de $[\![1, m]\!]$

Appli 17 Tirage de boules : Si on tire p boules dans une urne à m éléments :

1) Avec ordre, avec remise : m^p possibilités de combinaisons

2) Avec ordre, sans remise : A_m^p (Thm 15).

Ex 18 Apprabet braille (avec remise)

2^6 signes possibles

2) Combinaisons

Soit $k \in \mathbb{N}$, $1 \le k \le m$

Def 19 k-combinaison : k sous-ensemble de E

Nombre de combinaisons : $\binom{m}{k}$

Prop 20 $\binom{m}{p} = \frac{m!}{p!(m-p)!} = \binom{m}{m-p} = \binom{m-1}{p-1} + \binom{m-1}{p} = \frac{m}{p}\binom{m-1}{p-1}$

$$\binom{m}{p} = \frac{m}{m-p}\binom{m-1}{p} = \frac{m-p+1}{p}\binom{m}{p-1}$$

Prop-Def 21 Triangle de Pascal

	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

se construit géométriquement via $\binom{m}{p} = \binom{m-1}{p} + \binom{m-1}{p-1}$.

[De Biasi ch 2]

Prop 22 - Binôme de Newton

$\forall a,b \in \mathbb{C}, (a+b)^m = \sum_{0\leq p\leq m} a^p b^{m-p}$

Appli 23 Calcul de sommes

Si $y = 1+x$, $y^i = \sum_{0\leq j\leq i} \binom{i}{j} x^j$, $x^i = (y-1)^i = \sum_j \binom{i}{j}(-1)^{i-j} y^j$

$\sum_{m,p} = \sum_{1\leq k\leq m} k^p$, $\sum_{m,1} = \frac{(m+1)m}{2}$, $\sum_{m,2} = \frac{m(m+1)(m+2)}{6}$, ...

Lem 24 - Des bergers

Soit A, B deux ensembles finis, $\varphi : A \to B$

Si $\forall x \in B$, $|\varphi^{-1}(x)| = m$ alors $|A| = m|B|$

Appli 25 : on a m moutons, si on compte leur pattes et qu'on divise par 4, on obtient m.

[Cal]

III) Un peu de théorie des groupes

1) Définitions

Soit $(G,\times)$ un groupe, de neutre e. Soit E un ensemble non vide

Def 25 G opère à gauche sur E si il existe une application.

$\cdot : G\times E \to E$, $(g,x) \mapsto g.x$ tq $\forall (g,h) \in G, \forall x \in E$, $\begin{cases} gh \cdot x = g\cdot(h\cdot x) \\ e \cdot x = x \end{cases}$

Ex 26 1) Soit $H < G$, G opère à gauche sur $(G/H)_g$.

$G \times (G/H)_g \longrightarrow (G/H)_g$

$(g, xH) \longmapsto gxH$

2) G opère sur G : $G\times G \to G$, $(g,h) \mapsto ghg^{-1}$

Def 27 Stabilisateur de x. $G_x = \mathrm{Stab}_x = \{g\in G, g\cdot x = x\}$

Orbite de x : $\omega_x = \{g\cdot x, g\in G\}$

Ex 28 1) $G_{xH} = xHx^{-1}$

2) $G_x = \{g\in G, gxg^{-1} = x\} = Z_x(G)$

$\omega_x = \{gxg^{-1}, g\in G\}$

2) Applications au dénombrement

Thm 29 $\forall x \in E$, $|\omega_x| = [G : G_x]$

Cor 30 1) Soit G un groupe operant sur $\mathcal{P}(G)$ par conjugaison $\forall S \in \mathcal{P}(S)$, $|\omega_S| = [G : N_G(S)]$

2) Si $|E| < +\infty$, $|E| = \sum_{(x_i) \text{ rep des } G\text{-orbites}} [G : G_{x_i}]$

Thm 31 Formule de Burnside

Soit $g\in G$, X^g est l'ensemble des points fixes de E sous l'action de $\langle g\rangle$.

On note $|O|$ le nombre des orbites de E sous l'act° de G.

$$|O| = \frac{1}{|G|}\sum_{g\in G} |X^g|$$

[Ulm] voir dev

Appli 32 Dénombrement des coloriages des solides [DVT]

En particulier, pour le cube on a 57.

IV) Dénombrement sur les corps finis

1) Algèbre linéaire sur les corps finis

Prop 33 Cardinaux de groupes linéaires sur $\mathbb{F}_q$

$|GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i)$

$|SL_m(\mathbb{F}_q)| = \frac{|GL_m(\mathbb{F}_q)|}{|\mathbb{F}_q|} = \left[\prod_{i=0}^{m-1}(q^m-q^i)\right] / (q-1)$

$|SO(\mathbb{F}_p)| = \begin{cases} 2 & \text{si } p = 2 \\ p-1 & \text{si } p = 1\ [4] \\ p+1 & \text{si } p = 3\ [4] \end{cases}$

Prop 34 (avec des actions de groupes)

$\#\{A \in GL_m(\mathbb{F}_p), A^2 = I_m\} = \sum_{p=0}^{m} \frac{|GL_m(\mathbb{F}_p)|}{|GL_p(\mathbb{F}_p)|\,|GL_{m-p}(\mathbb{F}_p)|}$

[FGN AP1]

2) Fonctions arithmétiques et applications en dénombrement

Def 35 Indicatrice d'Euler de $m\in\mathbb{N}, m\geq 1$:

$\varphi(m) = \#\{m \in [\![1,m]\!], m \wedge m = 1\}$

Appli 36 Si $m = \prod_{1\leq i\leq k} p_i^{\alpha_i}$, $P_i = \{q \in [\![1,m]\!], p_i \mid q\}$

$\varphi(m) = m - |\bigcup_{1\leq i\leq k} P_i|$

Rem 37. Si p premier, $\varphi(p) = p-1$

• φ multiplicative : $\forall p,q$ premiers entre eux, $\varphi(p.q) = \varphi(p)\varphi(q)$.

mais ce n'est pas un morphisme.

Prop 38 Si p est premier, >3, $\alpha\in\mathbb{N}, \alpha\geq 2$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Appli 39 Chevalley - Warning Soit p un nombre premier, $\alpha \in \mathbb{N}^*$, $q = p^\alpha$

Soient $f_1, \dots, f_n \in \mathbb{F}_q[X_1,\dots,X_m]$ tq $\sum_{i=1}^{n} d^\circ f_i < m$

$\#\{(a_1,\dots,a_m) \in \mathbb{F}_q^m, \forall i \in [\![1,n]\!], f_i(a_1,\dots,a_m) = 0\} \equiv 0\ [p]$.

[De Biasi] [Pe] [Ra] [Cal] [Ra] [Zav]

[Pe]

Def 40 Fonction de Mobius

$\mu : \mathbb{N}^* \to \{0, 1, -1\}$, $\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré
$\mu(\prod_{i=1}^{r} p_i) = (-1)^r$ si p_i sont des nombres premiers distincts

Prop 41

1) μ est multiplicative : $\forall m, n \in \mathbb{N}, m \wedge n = 1 \Rightarrow \mu(m \cdot n) = \mu(m)\mu(n)$
2) $\forall n \in \mathbb{N}, n \geq 1, \sum_{d \mid n} \mu(d) = 0$

Cor 42 Formule d'inversion de Mobius $\Phi(n) = \sum_{d \mid n} \mu(\frac{n}{d}) d$.

Appli 43 Nombre de polynômes irréductibles de $\mathbb{F}_q[X]$ unitaire de degré n, noté $I(n, q)$:

$$I(n, q) = \frac{1}{n} \sum_{d \mid n} \mu(\frac{n}{d}) q^d.$$

[Dem]

Appli 44 : Algorithme de Berlekamp pour la cryptographie

3) Application en théorie des nombres

Def 45 Symbole de Legendre. Soit p un nombre premier impair
Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$, $(\frac{a}{p}) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^* \\ -1 & \text{sinon} \end{cases}$

Prop 46 $(\frac{a}{p}) = a^{\frac{p-1}{2}}$

Cor 47 Si $a \in \mathbb{F}_p^*$, $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + (\frac{a}{p})$

Thm 48 Loi de reciprocité quadratique [DVT]
Soit $q \in \mathbb{N}$, $q \geq 2$ premier, $p \neq q$. $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{q-1}{2} \frac{p-1}{2}}$

[Ha Ga TL]

Appli 49 Symbole de Jacobi
Soit $a, b \in \mathbb{N}$, $b = \prod_{\substack{p_i \text{ premier} \\ i=1}}^{r} p_i^{q_i}$, on définit le symbole de Jacobi :

$$(\frac{a}{b}) = \prod_{i=1}^{r} (\frac{a}{p_i})^{q_i}$$

Appli

II) Un peu de séries génératrices

Def 50 Soit $(a_n)_{n \in \mathbb{N}}$ une suite de réels
On définit la série génératrice de $(a_n)_n$ comme la série formelle $\sum_{n \in \mathbb{N}} a_n X^n \in \mathbb{R}[[X]]$

1) Applications et méthodes de dénombrement

Ex S1 $\sum_{a_1 + \dots + a_k = n} a_1 \cdots a_k = : C(n, k)$ avec $S(X) = \sum_{n \geq 1} n X^n$

$(S(X))^k = \sum_{n \geq 1} C(n, k) X^n$ d'où $C(n, k) = \binom{n+k-1}{2k-1}$

[De Biasi CA 3]

Ex S2 Le nombre de permutations de $[\![1, n]\!]$ est $n! = \sum_{0 \leq p \leq n} \frac{(-1)^p}{p!}$
par $S(X) = \sum_{n \geq 0} \frac{d_n}{n!} X^n$

Ex S3 Nombre u_n d'involution d'un n-ensemble
(ie. une permutation σ tq $\sigma^2 = id$)

$u_n = u_{n-1} + (n-1) u_{n-2}$ d'où $u_n = \sum_{p+2q=n} \frac{n!}{2^p p! q!}$

2) Nombres célèbres et applications

Appli 54 Nombre de Catalan. $b_n = \frac{1}{n+1} \binom{2n}{n}$.

via le développement de Taylor-Young de $\sqrt{1-4x}$ autour de 0.

[De biasi dfG]

Application : nombre d'arbre binaires différents sur un ensemble fini

[Cos] [FGNAP]

Appli 55 Nombre de Bell B_n : nombre de partitions de $[\![1, n]\!]$

$B_0 = 1$, $B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{n^k}{k!}$

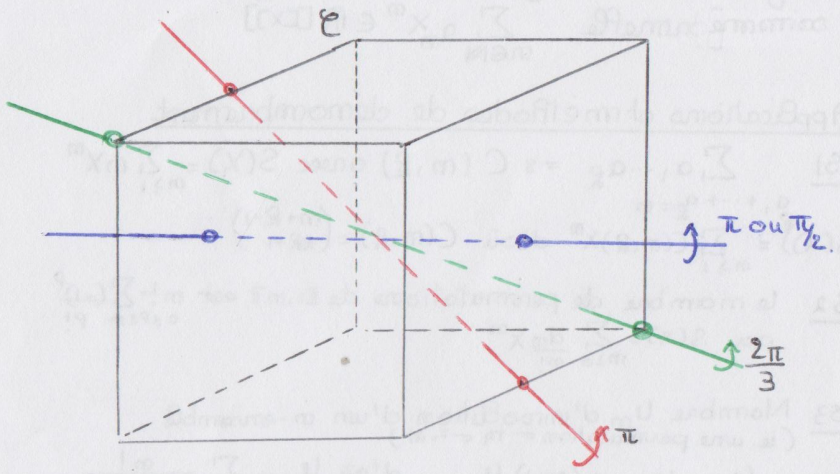
[FGN Ana 2]

Appli 56 Partition d'un entier à pas fixés

Soient $a_1, \dots, a_k \in \mathbb{N}^*$, $a_i \wedge a_j = 1$ $\forall i \neq j$
$\forall n \in \mathbb{N}^*$, $u_n = \#\{(x_1, \dots, x_k) \in \mathbb{N}^k, \sum_{i=1}^{k} a_i x_i = n\}$.

$u_n \underset{n \to +\infty}{\sim} \frac{1}{a_1 \cdots a_k} \frac{n^{k-1}}{(k-1)!}$

Annexe $\mathcal{G}_{Isom^+(\mathcal{C})} \cong C_4$



Bibliographie

[Gar] Olivier Garet, "De l'intégration aux probabilités" Ellipses

[De Biasi] Jean De Biasi, "Maths pour le CAPES et l'agrégation interne"

[Caf] : Josette Calais, Théorie des groupes

[Ulm] : Ulmer, Théorie des groupes

[FGN Alg1] : Oraux X-ENS, FGN Algèbre 1

[Per] : Perrin, cours d'algèbre

[Zav] : Zavidovique, Un max de maths

[Dem] : Demazure, cours d'algèbre

[H2G2T1] : Calvera Germoni, Histoire Redoutes de groupes et de géométrie tome 1

[Car] : Carmen, Introduction à l'algorithmique

[FGN Ana2] : Oraux X-ENS, FGN Analyse 2

[Combes] : Combes, Algèbre et géométrie

[Szpirglas] : Szpirglas, Algèbre L3.

Emily CLEMENT
Julien GABET

Isométrie du cube et applications

Emily Clement

Master 2 MEEF

Cadre :
On prend un cube (*i.e.* 12 arrêtes, 6 faces, 8 sommets, et r couleurs ($0 \leqslant r \leqslant 6$).
On va introduire des notations :

- $\mathcal{E}_3$ le $\mathbb{R}-$espace affine euclidien de dimension 3.
- $\mathrm{Isom}(\mathcal{C}) = \{f \in \mathcal{O}_3(\mathbb{R}) \,|\, f(\mathcal{C}) = \mathcal{C}\}$ le groupe des isométries affines de f
- $\mathrm{Isom}^+(\mathcal{C}) = \mathrm{Isom}(\mathcal{C}) \cap \{\det = 1\}$ le groupe des déplacements de f.

$\mathcal{O}_3(f)$ opère naturellement sur $\mathcal{E}_3$ par $f, A \mapsto f \cdot A$, $\mathrm{Isom}^+(f)$ est le stabilisateur de $\mathcal{O}_3^+(\mathbb{R})$ On numérote les grandes diagonales pour mieux expliquer les choses sur le dessin suivant : $(1), (2), (3), (4)$.
On va alors affirmer les deux choses suivantes :

Proposition .1

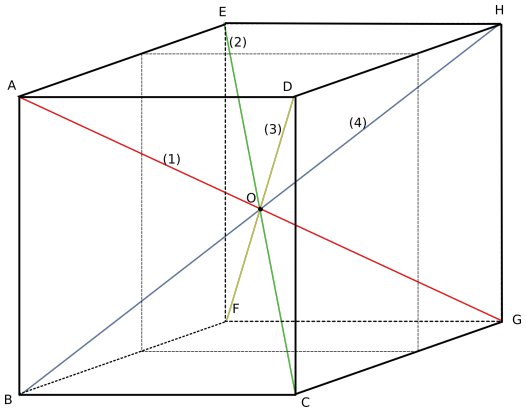
Soit $\mathcal{C}$ un cube, les isométries directes du cube est un groupe isomorphe à $\mathfrak{S}_4$.

Application :
Si on dispose de p couleurs, on a 57 manières différentes à isométries près de colorier un cube.
On se place avec un cube centré en le point O d'origine car cela ne change rien au problème. On va faire la démonstration en plusieurs étapes :

1. On montre l'existence d'un morphisme $\rho : \quad G \quad \rightarrow \quad \mathfrak{S}_4 \quad$ où $G = \mathrm{Isom}(\mathcal{C})$
2. on montre que $\rho_{|G^+}$ est injectif par étude du noyau
3. on montre qu'il est surjectif (donc bijectif) en cherchant les antécédents des éléments de $\mathfrak{S}_4$ géométriquement.
4. (Application) On utilise les actions de groupe pour dénombrer les points fixes par éléments de G^+
5. on applique Burnside pour calculer k le nombre de coloriage possible à isométrie directe près

Démonstration de la proposition

Étape 1 Soit f une isométrie, f préservant le cube, elle préserve les distances donc un segment réalisant le diamètre est envoyé sur un segment réalisant le diamètre, ici un dessin pour nommer les grandes diagonales du cube, $(1), (2), (3), (4)$:



On a ici 4 grandes diagonales, donc on peut considérer la restriction de l'action de G sur $\mathfrak{S}_4$ sur les 4 grandes diagonales. On pose rho le morphisme associé :

$$\rho : \quad G \quad \rightarrow \quad \mathfrak{S}_4$$

Étape 2

$\ker(\rho)$ est l'ensemble des isométries qui envoient (1) sur (1), (2) sur (2) etc, donc on a évidement l'identité et s_0 qui intervertit chaque sommets diagonalement opposés, mais cette transformation est de déterminant -1 donc :

$$\ker\left(\rho_{|G^+}\right) = \{\mathrm{Id}\}$$

en effet, si $\sigma \in \ker(\rho)$ tel que $\sigma \neq \mathrm{Id}$, alors il existe un sommet qui n'est pas envoyé sur lui-même, mettons que ce soit A.
Alors $\sigma([AG]) = [AG]$, donc comme les isométries préservent les barycentres, elle préservent les extrémités de segment donc $\sigma(A) = G$ et $\sigma(G) = A$.
De même, $\sigma(B) \in \{B, H\}$ par le même argument, or les distances étant préservé $\sigma([AB])$ est de même longueur que $[AB]$, donc on a en choix, pour que $\sigma(B)$ soit à distance de $[AB]$ de G :

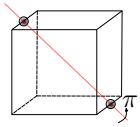
$$\sigma(B) \in \{F, C, H\}$$

donc $\sigma(B) = H$
De même $\sigma(C) = C$, or les vecteur OA, OB et OC formant une base de l'espace affine, on peut retrouver l'isométrie $\sigma = s_0$

Étape 3 Recherchons maintenant les antécédents de chaque éléments de $\mathfrak{S}_4$:

2−**cycles (transposition)**

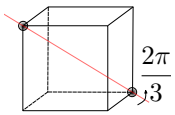
On a un éléments par exemple de la forme $\sigma = (12)$ correspond au rotations d'angle $\dfrac{\pi}{2}$ de d'axe passant par le milieu des arrêtes :
Ici les diagonales (1) et (2) restent inchangées et (3) est envoyées sur (4) et réciproquement, on a donc bien exhibé un 2−cycles.



On a 6 telles rotations différentes d'angle π (6 paires de deux arrêtes)

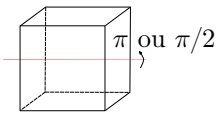
3−**cycles**

Un 3−cycle conserve la grande diagonale qui sert d'axe de rotation (4) d'angle $\dfrac{2\pi}{3}$, et la diagonale (1) est envoyée sur (3), (3) sur (2) et (2) sur (1). Cela forme un 3−cycle.



On a 8 telles rotations (2 par diagonales car on peut inverser l'angle et faire une rotation de $-2\pi/3$

4−**cycles**

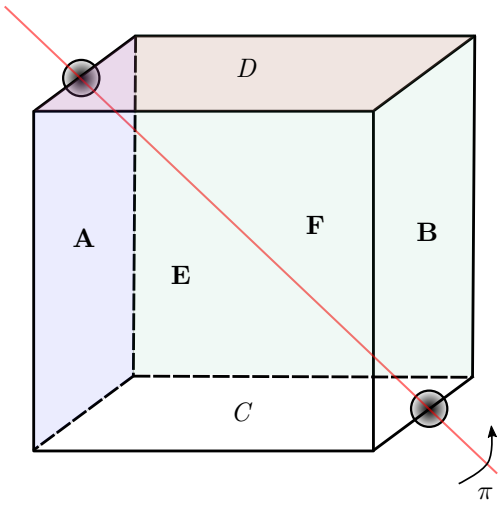


Un 4−cycle correspond à une rotation de $\pi/2$ avec comme avec de rotation les deux centres de deux faces opposées.
Ainsi avec un $\sigma = (1234)$, on envoie (1) sur (2), (2) sur (4), (4) sur (3) et (3) sur (1).
On a donc bien un 4−cycle avec cette transformation et 6 telle transformations.

Doubles transpositions On a le même raisonnement ici : $\sigma = (12)(34)$ envoie (1) sur (4), (4) sur (1), et (2) est envoyé sur (3) et réciproquement.

Étape 4 : On dénombre les points fixes par ces rotations :

- 2−**cycles** On a numéroté les faces ici pour une meilleure lisibilité :

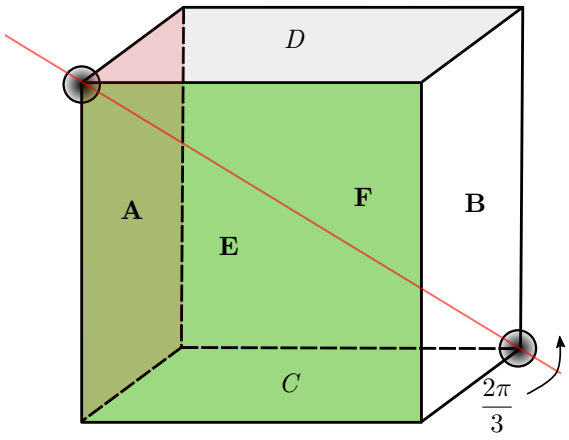


Avec cette rotation :

Face bleue A	↔	Face rouge D
Face B	↔	Face C
Face E	↔	Face F

On a donc p^3 coloriages possibles

- 3-**cycles** Si l'on colorie les faces du cube en gris, vert et rouge pour mieux visualiser :

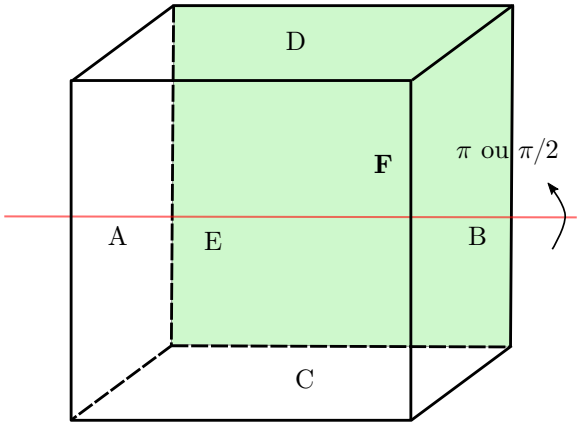


On a :

F. verte E → F. grise D → F. rouge A → F. verte E

Et on a la même chose pour le deuxième groupe de 3 faces, que l'on a pas colorié par soucis de lisibilité. Pour fixer le coloriage, on doit donc fixer deux groupes de faces : Le premier des faces en couleur sur le dessin, et le deuxième sans couleur.
On a donc p^2 coloriages possibles

- **4-cycles et doubles transpositions**



Pour les $4-$**cycles**, donc les rotations de $\frac{\pi}{2}$, la face **F** (verte et en bold pour moins d'ambiguïté avec la face de devant E) est envoyée sur la face C...en fait on va résumer par la suite suivante :

$$\begin{array}{ccccccccc} D & \to & F & \to & C & \to & E & \to & D \\ & & & & A & \leftrightarrow & A & & \\ & & & & B & \leftrightarrow & B & & \end{array}$$

et les faces A et B par lesquelles passent l'axe de rotations restent donc inchangées.
On peut donc choisir le coloriage de A, B et d'une des faces C, D, E, F, on fixe donc p^3 coloriages possibles
Pour **les doubles transpositions**, on a :

$$\begin{array}{ccc} D & \leftrightarrow & C \\ E & \leftrightarrow & F \\ A & \to & A \\ B & \to & B \end{array}$$

On fixe donc p^4 coloriages possibles.

Conclusion

Étape 5 : compter le nombre de coloriages possibles avec Burnside

On rappelle la formule de Burnside, si on note r le nombre d'orbites :

$$r = \left|\mathrm{Orb}_X\left(G^+\right)\right| = \frac{1}{|G|}\sum_{g\in G^+}\left|\mathrm{Fix}_X\left(g\right)\right|$$

Rotation	Nombre de rotations	Nombre de coloriages fixés par une rotations	Contribution à $\sum \lvert \mathrm{Fix}\,(g)\rvert$ dans le cas $p = 3$
Id	1	p^6	729
Axes par sommets diagonalement opposés, d'angle $\pm\dfrac{2\pi}{3}$	8	p^2	72
Axes par milieux des cotes opposés, d'angle π	6	p^3	162
Axes par centres des faces opposés, d'angle π	3	p^4	243
Axes par centres des faces opposés, d'angle $\dfrac{\pm\pi}{2}$	6	p^3	162
Total :	24		1368

D'où

$$\left|\mathrm{Orb}_X\left(G^+\right)\right| = \frac{1}{|G|}\sum_{g\in G^+}\left|\mathrm{Fix}_X\left(g\right)\right|$$

Si $p = 3$ par exemple, $\left|\mathrm{Orb}_X\left(G^+\right)\right| = \dfrac{1368}{24} = 57$.
Pour p couleurs quelconques, on a :

$$\frac{p^6 + p^2 + 2p^3 + p^4}{24}$$

coloriages possibles.
On a donc 57 manières différentes de colorier un cube en rouge, blanc et/ou bleu, par Burnside !

Questions sur ce développement

1. Pourquoi $\mathrm{Ker}\,\rho = \{\mathrm{Id}, s_0\}$? Lorsque nous considérons les isométries directes **et** indirectes, nous devons alors prendre en compte l'isométrie qui intervertit chaque sommets diagonalement opposés. Cette transformation est indirecte car de déterminant -1.
   On a donc ensuite $\mathrm{Ker}\left(\rho_{|G^+}\right) = \{\mathrm{Id}\}$ d'où l'injectivité.
2. Quelles est la différence entre retournement et renversement ? Le renversement est une symétrie par rapport à un hyperplan et un retournement une rotation d'angle π, c'est donc un déplacement.

Définition du symbole de Legendre : si $x \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, on définit :

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \\ -1 & \text{sinon} \end{cases}$$

Convention : $\left(\frac{0}{p}\right) = 0$

Lemme .1 (*H_2G_2 T1 p* 184)

Soit q un nombre premier impair, $a \in \mathbb{F}_q^*$,

$$\left|\left\{x \in \mathbb{F}_q, ax^2 = 1\right\}\right| = 1 + \left(\frac{a}{q}\right)$$

Théorème .1 (*Loi de réciprocité quadratique*)

Pour $q \in \mathbb{N}$, $q > 2$ un nombre premier, différent de p, on a la loi suivant :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

La preuve va consister à calculer le cardinal modulo p de la sphère suivante :

$$X = \left\{(x_1, \cdots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\right\}$$

pour obtenir les deux équations suivantes :

$$|X| = \left(\frac{p}{q}\right) = 1 \tag{A}$$

$$|X| = \left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^d, d = \frac{p-1}{2} \tag{M}$$

On les traduit ensuite par les symboles de Legendre via :

Lemme .2 (*H_2G_2 T1 p* 183)

Soit p un nombre premier, impair, et $q \in \mathbb{F}_p$, on a la caractérisation suivante :

$$\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}}.$$

Démonstration : • **Étape** 1 **: calcul de $|X|$ via les actions de groupes.**

$X \subset \mathbb{F}_q^p$ et $\frac{\mathbb{Z}}{p\mathbb{Z}} \curvearrowright \mathbb{F}_q^p$ par permutation cyclique :

$$\begin{array}{ccccc} \frac{\mathbb{Z}}{p\mathbb{Z}} & \times & \mathbb{F}_q^p & \to & \mathbb{F}_q^p \\ k & , & (x_1, \cdots, x_p) & \mapsto & (x_{1+k}, \cdots, x_{n+k}) \end{array}$$

où les indices sont vu modulo p, *i.e* : $x_{l+p} = x_l$.
$\text{Stab}_x = \left\{k \in \frac{\mathbb{Z}}{p\mathbb{Z}}, k \cdot \boldsymbol{x} = \boldsymbol{x}\right\}$
Orbite de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ dans X : soit $\boldsymbol{x} \in X$,
— Soit $\boldsymbol{x} = (x, \cdots, x) \in \mathbb{F}_q^p$, et $\text{Stab}_x = \frac{\mathbb{Z}}{p\mathbb{Z}}$
Nombre d'orbite de cette forme : c'est exactement les solutions de $px^2 = 1$.
Ce nombre d'équations vaut $1 + \left(\frac{p}{q}\right)$ par le lemme .1.

— Soit $\exists i \neq j$, $x_i \neq x_j$ et $\text{Stab}_x = e$ seulement, ces orbites sont de taille p.
Les orbite forment une partition de X, en sommant on a donc :

$$|X| = 1 + \left(\frac{p}{q}\right) \mod p$$

• **Étape 2 : Utilisation des matrices congruentes**
$d = \frac{p-1}{2}$, on considère $I_p, A \in \mathcal{M}_p(\mathbb{F}_q)$:

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}, A = \begin{pmatrix} B & & \\ & B & \\ & & \ddots \\ & & & a \end{pmatrix}$$

où $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $a = (-1)^{\frac{p-1}{2}} = (-1)^d$ On a les propriétés suivantes :
A et I_p sont **symétriques**, de rang p, de déterminant 1 donc de même discriminant)déterminant modulo les carrés) sur $\mathbb{F}_p$.
Elles sont donc congruentes, on a donc un changement de variable linéaire qui identifie X à :

$$X' = \left\{(y_1, \cdots, y_d, z_1, \cdots, z_d, t) \in \mathbb{F}_q^p, 2(y_1 z_1 + \cdots y_d z_d) + at^2 = 1\right\}$$

Comptons les différentes types de points :
— Si $y_1 = \cdots = y_d = 0$, les z_i sont donc quelconques ($q^d = q^{(p-1)/2}$ possibilités) et seul $at^2 = 1$ détermine les points ($1 + \left(\frac{a}{q}\right)$ possibilités par le lemme .1, donc en sommant : $q^{(p-1)/2}\left[1 + a^{(q-1)/2}\right] = \left[q^{(p-1)/2}\right]\left[1 + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}}\right]$ tels points.
— Si $\exists i$ tel que $y_i \neq 0$: on fixe $(y_1, \cdots, y_d)$ et t ($q^d - 1$ choix pour y_i et q pour t) on doit alors choisir $z_1, \cdots, z_d$ dans $\mathbb{F}_q^d$ tels que l'équation est vérifiée, c'est donc choisir cet ensemble de point dans un hyperplan affine de $\mathbb{F}_q^d$: q^{d-1} choix.
On a donc $\left(q^d - 1\right) \cdot q \cdot q^{d-1} = \left(q^{(p-1)/2} - 1\right) q^{(p-1)/2}$ tels points.
En sommant on obtient :

$$|X| = \left[q^{(p-1)/2}\right]\left[1 - 1 + q^{(p-1)/2} + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}}\right]$$

Soit :

$$|X| = q^{(p-1)/2}\left(q^{(p-1)/2} + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}}\right)$$

En combinant les deux équations, on a :

$$q^{(p-1)/2}\left(+q^{(p-1)/2} + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}}\right) = 1 + \left(\frac{p}{q}\right) \mod p$$

Soit :

$$\left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}}\right) = 1 + \left(\frac{p}{q}\right) \mod p$$

En multipliant par $\left(\frac{p}{q}\right)$, comme un symbole de Legendre au carré vaut forcément 1, on obtient la loi de réciprocité quadratique :

$$\cancel{\left(\frac{q}{p}\right)} + (-1)^{\frac{(p-1)(q-1)}{2\cdot 2}} = \cancel{\left(\frac{q}{p}\right)} + \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \mod p$$

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}}$$

■