Le théorème de Pólya

S. Baumard et A. Page

Résumé

Le théorème de Pólya est un outil combinatoire permettant le dénombrement des coloriages d'ensembles à l'action d'un groupe près. après avoir rappelé les bases de la théorie des actions de groupes, on expose une preuve de ce théorème et on en examine quelques conséquences pour certains polytopes réguliers ainsi que pour la droite projective sur un corps fini. La première partie est une adaptation libre de [Big89].

La lecture de l'exemple du paragraphe 2.2 nécessite de connaître les notions de corps fini (voir par exemple [Dem97]) et de droite projective (voir [Aud06] ou [Sam86] pour un point de vue géométrique).

0 Préliminaires

Soient G un groupe et X un ensemble. Une *action* de G sur X est une application $\cdot : G \times X \to X$ telle que $1 \cdot x = x$ pour tout $x \in X$ et que $g \cdot (h \cdot x) = (gh) \cdot x$ pour tous éléments $x \in X$ et $g, h \in G$. Cela revient à se donner un morphisme de groupes de G dans le groupe $\mathfrak{S}(X)$ des permutations de X. On notera souvent $G \circlearrowright X$.

Exemple. Le groupe $\mathrm{SO}_3(\mathbb{R})$ des rotations de l'espace agit sur $\mathbb{R}^3$ de façon naturelle.

Soit G un groupe agissant sur un ensemble X. On dit qu'un élément $g \in G$ *fixe* un point $x \in X$, ou que x est un *point fixe* de g, si $g \cdot x = x$. Pour $x \in X$, le *stabilisateur* $\mathrm{Stab}(x)$ est le sous-groupe des éléments $g \in G$ qui fixent le point x. Pour $g \in G$, le *fixateur* $\mathrm{Fix}(g)$ est le sous-ensemble des points fixes de g.

Exemple. Dans l'action de $\mathrm{SO}_3(\mathbb{R})$ sur $\mathbb{R}^3$, le stabilisateur d'un vecteur unitaire s'identifie à $\mathrm{SO}_2(\mathbb{R})$ (en complétant ce vecteur en une base orthonormée directe, les matrices le stabilisant se décomposent par blocs), et le fixateur d'une rotation non triviale est une droite (l'axe de la rotation en question).

Dans une action $G \circlearrowright X$, l'*orbite* d'un point x sous le groupe G est l'ensemble $G \cdot x = \{g \cdot x \mid g \in G\}$. Deux orbites sont soit disjointes soit confondues ; les orbites forment donc une partition de X. On appelle *quotient de X sous l'action de G* l'ensemble X/G de ces orbites.

Exemple. Les orbites de $\mathbb{R}^3$ sous l'action de $\mathrm{SO}_3(\mathbb{R})$ sont exactement les sphères centrées en l'origine, et le quotient $\mathbb{R}^3/\mathrm{SO}_3(\mathbb{R})$ s'identifie à $\mathbb{R}^+$ en envoyant une sphère sur son rayon.

Supposons qu'un groupe fini G agisse sur un ensemble X. Toutes les orbites sont alors finies, et l'orbite d'un point x est de cardinal $\frac{|G|}{|\operatorname{Stab} x|}$: en effet, dans l'application naturelle qui envoie G dans $G \cdot x$, la préimage de chaque point est en bijection avec $\mathrm{Stab}(x)$.

Étant donnés une action $G \curvearrowright X$ et un ensemble Y, les applications $f : X \to Y$ constantes sur les orbites (ou, de façon équivalente, vérifiant $f(g \cdot x) = f(x)$ pour tous g et x) correspondent aux applications $\bar{f} : X/G \to Y$ en posant $\bar{f}(G \cdot x) = f(x)$. On fera souvent l'abus de notation consistant à identifier f et $\bar{f}$.

Exemple. Soit $f = \|\cdot\|^2 : \mathbb{R}^3 \to \mathbb{R}$. Cette application est constante sur les orbites sous $\mathrm{SO}_3(\mathbb{R})$. L'application correspondante $\bar{f} : \mathbb{R}^3/\mathrm{SO}_3(\mathbb{R}) \to \mathbb{R}$ est le carré du rayon.

Si $G \curvearrowright X$ et si $g \in G$, le sous-groupe $\langle g \rangle$ de G engendré par g agit encore sur X, et l'orbite d'un point $x \in X$ est l'ensemble des $g^n \cdot x$ pour $n \in \mathbb{Z}$. Si X est fini, g agit comme une permutation, et la partition de X en orbites sous $\langle g \rangle$ correspond à la décomposition en cycles de cette permutation.

1 Le théorème

Problème. On considère un groupe fini G agissant sur un ensemble fini X, et on s'intéresse aux coloriages de X essentiellement distincts, c'est-à-dire qu'on considère deux coloriages comme identiques dès qu'on peut obtenir l'un à partir de l'autre en faisant agir un élément de G. On aimerait connaître le nombre de coloriages de X essentiellement distincts utilisant un nombre de couleurs donné, ou utilisant chaque couleur un nombre de fois donné.

Pour se rendre compte de la puissance du théorème de Pólya, il est utile de commencer par faire quelques comptages à la main.

Exercice. On s'intéresse au dodécaèdre régulier, c'est-à-dire l'unique polyèdre régulier à douze faces (voir figure 1 ci-dessous).

- De combien de manières peut-on colorier un dodécaèdre régulier fixé (on ne peut pas le tourner) avec deux couleurs ?
- De combien de manières peut-on colorier un dodécaèdre régulier avec deux faces noires et dix faces blanches, à rotation près ?
- De combien de manières peut-on colorier un dodécaèdre régulier avec une face rouge, deux faces noires et neuf faces blanches, à rotation près ?

Le théorème de Pólya fournit un moyen systématique et efficace de répondre à ce type de questions, épargnant le comptage à la main.

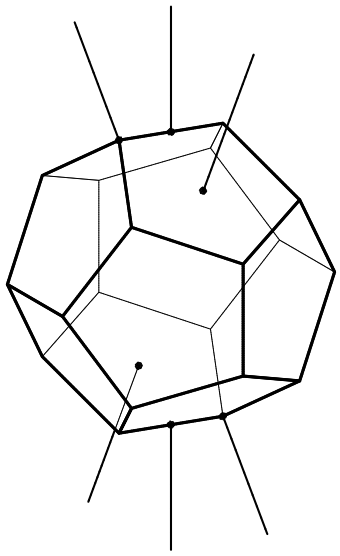

FIGURE 1 – Dodécaèdre régulier avec trois axes de rotation

On commence par démontrer un lemme classique sur les actions de groupes finis, qui sera la clef de voûte de la preuve du théorème de Pólya.

Lemme 1 (formule de Burnside pondérée)**.** *Soient G un groupe fini agissant sur un ensemble fini X, E un $\mathbb{Q}$-espace vectoriel*[1] *et $f : X/G \to E$ une application. Alors*

$$\sum_{\omega \in X/G} f(\omega) = \frac{1}{|G|} \sum_{g \in G} \sum_{\xi \in \operatorname{Fix} g} f(\xi).$$

Démonstration. L'idée consiste à sommer de deux façons différentes la fonction qui à $(g, \xi) \in G \times X$ associe $\mathbb{1}_{g \cdot \xi = \xi} f(\xi)$. D'une part

$$\sum_{(g,\xi) \in G \times X} \mathbb{1}_{g \cdot \xi = \xi} f(\xi) = \sum_{g \in G} \sum_{\xi \in X} \mathbb{1}_{g \cdot \xi = \xi} f(\xi) = \sum_{g \in G} \sum_{\xi \in \operatorname{Fix} g} f(\xi)$$

et d'autre part

$$\begin{aligned} \sum_{(g,\xi) \in G \times X} \mathbb{1}_{g \cdot \xi = \xi} f(\xi) &= \sum_{\xi \in X} \Big(\sum_{g \in G} \mathbb{1}_{g \cdot \xi = \xi} \Big) f(\xi) \\ &= \sum_{\xi \in X} |\operatorname{Stab} \xi| \, f(\xi) \\ &= \sum_{\xi \in X} \frac{|G|}{|G \cdot \xi|} f(G \cdot \xi) \quad \text{car } f \text{ est constante sur les orbites} \end{aligned}$$

1. Cet énoncé reste vrai en supposant seulement que E est un monoïde commutatif, en multipliant l'égalité par $|G|$.

$$= \sum_{\omega \in X/G} |\omega| \frac{|G|}{|\omega|} f(\omega) \quad \text{en regroupant les termes}$$
$$= |G| \sum_{\omega \in X/G} f(\omega)$$

d'où le résultat. □

Dans toute la suite, on considère un ensemble fini X à n éléments, sur lequel agit un groupe fini G. On se donne aussi un ensemble K de cardinal k, dont les éléments, notés $x_1, \ldots, x_k$, seront vus à la fois comme des couleurs et comme des variables formelles ; cette ambivalence est précisée par les définitions suivantes.

Définition (indicatrice des cycles)**.** Si $g \in G$, on appelle *indicatrice des cycles* de g le polynôme de $\mathbb{Z}[t_1, \ldots, t_n]$ défini par $\zeta_g = \prod_{\omega \in X/\langle g \rangle} t_{|\omega|}$. On a alors $\zeta_g = t_1^{\alpha_1} \cdots t_n^{\alpha_n}$, où α_i est le nombre d'orbites de cardinal i dans X sous l'action du sous-groupe $\langle g \rangle$ engendré par g. De même, on appelle indicatrice des cycles de G le polynôme $Z_{G \circlearrowright X} = \frac{1}{|G|} \sum_{g \in G} \zeta_g$. Bien que ces indicatrices dépendent de l'action de G sur X et pas uniquement du groupe G, on notera souvent $Z_G = Z_{G \circlearrowright X}$ quand le contexte empêchera toute ambigüité.

Exemple. Considérons G l'ensemble des rotations qui laissent globalement invariant le dodécaèdre régulier ; ce groupe agit naturellement sur l'ensemble X des faces de ce dodécaèdre. Soit ρ une rotation d'axe passant par deux centres de faces opposées du dodécaèdre et d'angle $\frac{2\pi}{5}$, qui est bien dans G. alors ρ fixe les deux faces opposées par lesquelles passe son axe, et les dix faces restantes forment deux couronnes de cinq faces que ρ fait tourner en décalant chaque face sur sa voisine. Ces deux couronnes forment donc chacune une orbite sous $\langle \rho \rangle$. Cette rotation agissant sur X possède finalement deux points fixes et deux orbites de cardinal 5, d'où $\zeta_\rho = t_1^2 t_5^2$.

Exercices.

- On fait agir $\mathfrak{S}_n$ par permutation sur $[\![1, n]\!]$. Que vaut l'indicatrice des cycles d'une permutation ?
- On se donne deux groupes G_1 et G_2 agissant respectivement sur des ensembles X_1 et X_2. Cela donne une action de $G_1 \times G_2$ sur la réunion disjointe $X_1 \sqcup X_2$ par $(g_1, g_2) \cdot x_1 = g_1 \cdot x_1$ si $x_1 \in X_1$ et $(g_1, g_2) \cdot x_2 = g_2 \cdot x_2$ si $x_2 \in X_2$. Montrer que $\zeta_{(g_1, g_2)} = \zeta_{g_1} \zeta_{g_2}$ pour tout $(g_1, g_2) \in G_1 \times G_2$, et que $Z_{G_1 \times G_2 \circlearrowright X_1 \sqcup X_2} = Z_{G_1 \circlearrowright X_1} Z_{G_2 \circlearrowright X_2}$.
- Soit G un groupe agissant sur X. On note N l'intersection des stabilisateurs des points de X, qui agit sur G par multiplication à gauche. Montrer que G/N est encore un groupe agissant sur X et que $Z_{(G/N) \circlearrowright X} = Z_{G \circlearrowright X}$. De même, si S est l'image de G dans $\mathfrak{S}(X)$, on a $Z_{S \circlearrowright X} = Z_{G \circlearrowright X}$.

Définition (coloriage)**.** On appelle *coloriage de X à k couleurs* (ou encore *coloriage à valeurs dans K*) de X toute application $\gamma : X \longrightarrow K$, et on note Γ

l'ensemble des coloriages à k couleurs de X, les ensembles X et K étant sous-entendus.

On dispose de deux actions naturelles sur Γ : celle de $\mathfrak{S}(K)$ par postcomposition des applications, et celle de G par $g \cdot \gamma = \gamma \circ g^{-1}$. Notre objectif sera de compter les coloriages de X à l'action de G près, deux coloriages étant équivalents modulo G s'ils sont envoyés l'un sur l'autre par un élément de G.

Exemple. Considérons un dodécaèdre posé sur une face, avec une face tournée vers l'observateur, X l'ensemble de ses faces et G son groupe de rotations. On prend comme ensemble de couleurs $K = \{n, r, b\}$ (noir, rouge, blanc). Soit γ le coloriage de X tel que les deux faces verticalement opposées soient noires, la face supérieure tournée vers l'observateur rouge et toutes les autres blanches.

Soit $\sigma \in \mathfrak{S}(K)$ qui échange n et b et qui laisse r inchangé. alors $\sigma \circ \gamma$ est le coloriage tel que les deux faces verticalement opposées soient blanches, la face supérieure tournée vers l'observateur rouge et toutes les autres noires.

Soit ρ la rotation d'axe vertical et d'angle $\frac{2\pi}{5}$ dans le sens trigonométrique (vu du dessus). alors $\rho \cdot \gamma = \gamma \circ \rho^{-1}$ est le coloriage tel que les deux faces verticalement opposées soient noires, la face supérieure à droite de celle tournée vers l'observateur rouge et toutes les autres blanches.

Définitions (indicatrice d'un coloriage, fonction génératrice des coloriages)**.** Pour $\gamma \in \Gamma$, on pose $\operatorname{ind} \gamma = \prod_{\xi \in X} \gamma(\xi) \in \mathbb{Z}[K]$. On a alors $\operatorname{ind} \gamma = x_1^{c_1} \cdots x_k^{c_k}$ où c_i est le nombre d'éléments de X de couleur $x_i \in K$. La fonction ind est constante sur les orbites de Γ sous G, et se factorise donc en une application encore notée $\operatorname{ind} : \Gamma/G \longrightarrow \mathbb{Z}[x_1, \ldots, x_k]$. Si A est une partie de Γ ou de Γ/G, on appelle *fonction génératrice des coloriages par* A le polynôme $U_A = \sum_{\gamma \in a} \operatorname{ind} \gamma \in \mathbb{Z}[K]$.

De même que $\operatorname{ind} \gamma$ encode le type du coloriage γ, la fonction génératrice U_A encode le nombre de coloriages de chaque type contenus dans A. Dans le cas où A est une partie de Γ/G, on compte les types des coloriages à l'action de G près.

Exemple. Avec les notations de l'exemple précédent, le coloriage γ utilise la couleur noire sur deux faces, la couleur rouge sur une face et la couleur blanche sur les neuf faces restantes. On a donc $\operatorname{ind} \gamma = b^9 n^2 r$. Avec les notations utilisées dans le cas général ($n = x_1$, $r = x_2$, $b = x_3$) cela donne $\operatorname{ind} \gamma = x_1^2 \, x_2 \, x_3^9$.

Remarque. La fonction génératrice $U_{\Gamma/G}$ est un polynôme symétrique en les éléments x_i de K. En effet, si $\sigma \in \mathfrak{S}(K)$, σ permute Γ/G car son action sur Γ commute avec celle de G : pour $g \in G$ et $\gamma \in \Gamma$, on a $g \cdot (\sigma \circ \gamma) = \sigma \circ \gamma \circ g^{-1} = \sigma \circ (g \cdot \gamma)$. Par conséquent,

$$\begin{aligned} \sigma \cdot U_{\Gamma/G} &= \sigma \cdot \sum_{\omega \in \Gamma/G} \operatorname{ind} \omega \\ &= \sum_{\omega \in \Gamma/G} \prod_{\xi \in X} \sigma(\omega(\xi)) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\omega\in\Gamma/G} \prod_{\xi\in X} (\sigma\circ\omega)(\xi) \\
&= \sum_{\omega\in\Gamma/G} \prod_{\xi\in X} \omega(\xi) \\
&= U_{\Gamma/G}.
\end{aligned}
$$

On sait donc par avance que $U_{\Gamma/G}$ est un polynôme à coefficients rationnels en les fonctions puissances définies par $\tau_i = x_1^i + \cdots + x_k^i$.

Notre objectif est de calculer $U_{\Gamma/G}$, dont les coefficients donnent, pour toute répartition de couleurs, le nombre de coloriages de X distincts modulo G qui ont cette répartition. Cet objectif est atteint par le résultat suivant, qui fournit explicitement l'écriture de $U_{\Gamma/G}$ en termes des fonctions puissances.

Théorème 2 (George Pólya, 1935)**.** *Soient G un groupe fini agissant sur un ensemble X de cardinal n, et k un entier naturel. On a l'identité polynomiale*

$$U_{\Gamma/G}(x_1,\ldots,x_k) = Z_{G\circlearrowright X}(\tau_1,\ldots,\tau_n).$$

Corollaire. Sous les mêmes hypothèses, le nombre de coloriages de X à k couleurs modulo l'action de G vaut $|\Gamma/G| = Z_{G\circlearrowright X}(k,\ldots,k)$.

Démonstration (du corollaire). On particularise le théorème en $\underline{x} = (1,\ldots,1)$ qui donne $\tau_i = k$ pour tout i. Cela donne $U_{\Gamma/G}(1,\ldots,1) = Z_{G\circlearrowright X}(k,\ldots,k)$. De plus $U_{\Gamma/G}(1,\ldots,1) = \sum_{\gamma\in\Gamma/G} 1^n = |\Gamma/G|$, ce qui conclut. □

Exemples. Reprenons la question : « De combien de manières peut-on colorier un dodécaèdre régulier avec une face rouge, deux faces noires et neuf faces blanches, à rotation près ? » On utilise encore les mêmes notations que dans les exemples précédents pour X et G. Nous démontrerons dans la partie 2.1 que l'indicatrice des cycles du groupe du dodécaèdre agissant sur ses faces est

$$Z_G = \tfrac{1}{60}(t_1^{12} + 24\,t_1^2\,t_5^2 + 15\,t_2^6 + 20\,t_3^4).$$

On applique alors le théorème de Pólya : $U_{\Gamma/G} = Z_G(\tau_1,\ldots,\tau_5)$ qui devient

$$\tfrac{1}{60}\big((r+n+b)^{12}+24\,(r+n+b)^2\,(r^5+n^5+b^5)^2+15\,(r^2+n^2+b^2)^6+20\,(r^3+n^3+b^3)^4\big).$$

On veut trouver le coefficient de $r\,n^2\,b^9$ dans cette expression. Cela revient à trouver le coefficient de $r\,n^2$ dans

$$\tfrac{1}{60}\big((r+n+1)^{12}+24\,(r+n+1)^2\,(r^5+n^5+1)^2+15\,(r^2+n^2+1)^6+20\,(r^3+n^3+1)^4\big).$$

Les termes $(r^2+n^2+1)^6$ et $(r^3+n^3+1)^4$ ne contiennent que des puissances trop grandes de r et n. Le terme $(r+n+1)^2\,(r^5+n^5+1)^2$ est égal à $(1+r+n)^2$ plus

des termes de trop grand degré, et aucun ne contient le monôme $r\,n^2$. Enfin, on a

$$\begin{aligned}(r+n+1)^{12} &= \cdots + \tbinom{12}{3}\,(r+n)^3 + \cdots \\ &= \cdots + 220\,(r+n)^3 + \cdots \\ &= \cdots + 220\cdot 3\,r\,n^2 + \cdots\end{aligned}$$

et le coefficient recherché est $\frac{220\cdot 3}{60} = 11$. Il existe donc 11 coloriages à une face rouge et deux faces noires, ce qu'on pouvait trouver par un comptage laborieux.

On trouve dans ce polynôme la solution à toutes les questions du même type avec trois couleurs. Par exemple, résolvons la question « De combien de manières peut-on colorier un dodécaèdre régulier avec deux faces rouge, cinq faces noires et cinq faces blanches, à rotation près ? », ce qui paraît difficile à compter à la main. Le terme $(r^2+n^2+1)^6$ (resp. $(r^3+n^3+1)^4$) ne contient que des monômes dont les puissances de r et n sont paires (resp. multiples de 3). Par ailleurs on a

$$\begin{aligned}(r+n+1)^2\,(r^5+n^5+1)^2 &= (r+n+1)^2\,(1+2\,n^5) + \cdots \\ &= \cdots + 2\,r^2\,n^5 + \cdots \\ \text{et}\qquad (r+n+1)^{12} &= \cdots + \tbinom{12}{5}\,(r+n)^7 + \cdots \\ &= \cdots + 792\,(r+n)^7 + \cdots \\ &= \cdots + 792\cdot 21\,r^2\,n^5 + \cdots,\end{aligned}$$

le coefficient recherché est donc finalement $\frac{792\cdot 21+24\cdot 2}{60} = 278$. Il semble difficile de trouver les 278 coloriages sans utiliser le théorème !

Le lemme technique que voici sera utile dans la preuve du théorème de Pólya.

Lemme 3. *Soit $\coprod_{j=1}^{p} X_j$ une partition de X. Soit $A \subset \Gamma$ l'ensemble des coloriages constants sur chaque X_j, et $m_j = |X_j|$. Alors*

$$U_A(x_1,\ldots,x_k) = \prod_{j=1}^{p} \tau_{m_j}.$$

Démonstration. Les coloriages constants sur chaque X_j s'identifient aux applications de $\{X_j \mid j \in [\![1,p]\!]\}$ dans K, et donc aux suites de p éléments de K. Par conséquent

$$\begin{aligned}U_A &= \sum_{\gamma\in a} \operatorname{ind}\gamma \\ &= \sum_{\gamma\in a}\prod_{\xi\in X}\gamma(\xi) \\ &= \sum_{\gamma\in a}\prod_{j=1}^{p}\gamma(X_j)^{m_j}\end{aligned}$$

$$= \sum_{1 \leqslant i_1, \ldots, i_p \leqslant k} \prod_{j=1}^{p} x_{i_j}^{m_j} \qquad \text{en posant } \gamma(X_j) = x_{i_j}$$
$$= \prod_{j=1}^{p} \sum_{i=1}^{k} x_i^{m_j}$$
$$= \prod_{j=1}^{p} \tau_{m_j}$$

ce qui est le résultat annoncé. □

Exemple. On dispose d'un dé à six faces numérotées de 1 à 6 par des points. On veut colorier chaque point en rouge ou en noir de manière à ce que les points d'une même face soient de la même couleur, et de sorte à obtenir 10 points rouges et 11 points noirs. On cherche à savoir de combien de façons différentes on peut procéder à un tel coloriage.

L'ensemble des points étant partitionné en six classes (les faces), on est dans la situation du lemme 3, qui donne pour fonction génératrice $U_A = \prod_{i=1}^{6}(n^i + r^i)$. Le nombre recherché est le coefficient de $n^{11}\, r^{10}$ dans U_A, qui vaut 5.

Pour prouver le théorème, on se servira aussi du lemme simple suivant.

Lemme 4. *Soient $\gamma \in \Gamma$ et $g \in G$. Alors $\gamma \in \operatorname{Fix} g$ si et seulement si γ est constante sur chaque orbite de $X/\langle g \rangle$.*

Démonstration. Si γ est constante sur ces orbites, alors, pour tout point $\xi \in X$, on a $(g{\cdot}\gamma)(\xi) = \gamma(g^{-1}{\cdot}\xi) = \gamma(\xi)$ car $g^{-1}{\cdot}\xi$ est dans l'orbite de ξ ; donc $\gamma \in \operatorname{Fix} g$.

Réciproquement, si $\gamma \in \operatorname{Fix} g$, soient ξ, ξ' dans la même orbite de X sous l'action de g. alors il existe un entier m tel que $\xi' = g^m \cdot \xi$, d'où $\gamma(\xi') = \gamma(g^m \cdot \xi) = (g^{-m} \cdot \gamma)(\xi) = \gamma(\xi)$ car $\gamma \in \operatorname{Fix} g$; donc γ est constante sur chaque orbite. □

Démonstration (du théorème). On applique la formule de Burnside généralisée pour l'action de G sur Γ, avec $E = \mathbb{Q}[K]$ et $f = \operatorname{ind}$: elle donne

$$U_{\Gamma/G} = \sum_{\omega \in \Gamma/G} \operatorname{ind} \omega = \frac{1}{|G|} \sum_{g \in G} \sum_{\gamma \in \operatorname{Fix} g} \operatorname{ind} \gamma.$$

De plus, si $g \in G$, l'action de g sur X induit une partition de X en orbites, ce qui donne l'ensemble $A_g \subset \Gamma$ des coloriages constants sur les orbites, qui est

égal à $\operatorname{Fix} g$ d'après le lemme 4. Donc

$$\begin{aligned} U_{\Gamma/G} &= \frac{1}{|G|} \sum_{g \in G} \sum_{\gamma \in \operatorname{Fix} g} \operatorname{ind} \gamma \\ &= \frac{1}{|G|} \sum_{g \in G} U_{\operatorname{Fix} g} \\ &= \frac{1}{|G|} \sum_{g \in G} U_{A_g} \qquad \text{par la remarque précédente} \\ &= \frac{1}{|G|} \sum_{g \in G} \prod_{\omega \in X/\langle g \rangle} \tau_{|\omega|} \quad \text{par le lemme 3} \end{aligned}$$

et finalement

$$U_{\Gamma/G}(x_1, \ldots, x_k) = Z_{G \circlearrowright X}(\tau_1, \ldots, \tau_n)$$

ce qui est l'énoncé du théorème de Pólya. □

2 Exemples de calcul

2.1 Coloriages de polytopes réguliers

On va calculer les indicatrices de cycles des groupes de symétries des polygones et des polyèdres réguliers, et en déduire certains nombres de colorations des sommets[2] de ces polytopes. Par définition, le groupe des symétries d'un polytope régulier est l'ensemble des rotations le stabilisant globalement, et agit naturellement sur l'ensemble des sommets dudit polytope.

On notera φ la fonction indicatrice d'Euler, définie par $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, et $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$, isomorphe (de façon non unique) à $\mathbb{Z}/n\mathbb{Z}$.

Théorème 5. *Les indicatrices de cycles correspondant correspondant à l'action des groupes de symétries des polytopes réguliers en dimension* 2 *et* 3 *sont résumées dans le tableau 1 page suivante.*

Démontrons le théorème.

- **Action des rotations sur le n-gone.** Le groupe G des rotations du polygone régulier à n côtés est isomorphe à $\mathbb{U}_n$, et l'ensemble X des sommets est aussi en bijection avec $\mathbb{U}_n$; en choisissant convenablement cet isomorphisme et cette bijection, l'action de G sur X se traduit simplement par l'action de $\mathbb{U}_n$ sur lui-même par multiplication. Le groupe $\mathbb{U}_n$ contient, pour tout diviseur d de n, exactement $\varphi(d)$ éléments d'ordre d, qui engendrent le sous-groupe $\mathbb{U}_d$. Pour l'action de ce sous-groupe, chaque orbite dans X est en bijection avec $\mathbb{U}_d$ qui est d'ordre d, et il y a donc $\frac{n}{d}$ orbites de même cardinal d.

2. Par dualité, on peut aussi en déduire le nombre de colorations des faces.

Groupe	Polytope	Indicatrice des cycles
C_n	n-gone	$\frac{1}{n}\sum_{d\mid n}\varphi(d)\,t_d^{n/d}$
D_n	n-gone	$\frac{1}{2}\,Z_{C_n} + \begin{cases}\frac{1}{4}(t_2^{n/2}+t_1^2\,t_2^{n/2-1}) & \text{si } n \text{ est pair}\\ \frac{1}{2}\,t_1\,t_2^{(n-1)/2} & \text{si } n \text{ est impair}\end{cases}$
S_t	tétraèdre	$\frac{1}{12}(t_1^4+8\,t_1t_3+3\,t_2^2)$
S_o	octaèdre	$\frac{1}{24}(t_1^6+6\,t_1^2\,t_4+3\,t_1^2\,t_2^2+6\,t_2^3+8\,t_3^2)$
S_c	cube	$\frac{1}{24}(t_1^8+8\,t_1^2\,t_3^2+9\,t_2^4+6\,t_4^2)$
S_i	icosaèdre	$\frac{1}{60}(t_1^{12}+24\,t_1^2\,t_5^2+15\,t_2^6+20\,t_3^4)$
S_d	dodécaèdre	$\frac{1}{60}(t_1^{20}+20\,t_1^2\,t_3^6+15\,t_2^{10}+24\,t_5^4)$

TABLE 1 – Cas des polytopes

Remarque. Le même argument donne, pour tout groupe G d'ordre n agissant sur lui-même par translation,

$$Z_{G\circlearrowright G} = \frac{1}{n}\sum_{d\mid n}\varphi_G(d)\,t_d^{n/d}$$

où $\varphi_G(d)$ est le nombre d'éléments de G d'ordre d.

• **Action du groupe diédral sur le n-gone.** Soit D_n le sous-groupe du groupe des isométries planes $\mathrm{O}_2(\mathbb{R})$, conservant le polygone régulier à n côtés, agissant sur l'ensemble X des sommets de ce polygone. Le groupe D_n est de cardinal $2n$, et contient C_n. Les autres éléments de D_n sont des réflexions, il suffit donc de trouver leurs axes.

Si n est *impair*, chaque axe passe par l'un des n sommets du polygone, et la réflexion associée a un point fixe : c'est le côté opposé au sommet par lequel son axe passe. Les autres orbites sont de cardinal 2, donc il y en a $\frac{n-1}{2}$. De plus, il y a n telles réflexions. Donc

$$Z_{D_n} = \tfrac{1}{2n}\,(n\,Z_{C_n} + n\,t_1\,t_2^{(n-1)/2}).$$

Si n est *pair*, chaque axe passe soit par deux sommets opposés du polygone, soit par deux milieux de côtés opposés du polygone, et il y a dans chacun de ces cas $\frac{n}{2}$ telles réflexions. Dans le premier cas, la réflexion n'a pas de point fixe et a donc $\frac{n}{2}$ orbites de cardinal 2. Dans le second cas, la réflexion a deux points fixes,

qui sont les deux côtés par lesquels l'axe passe, et $\frac{n}{2} - 1$ orbites de cardinal 2. Donc

$$Z_{D_n} = \frac{1}{2n}\left(n\, Z_{C_n} + \frac{n}{2}\, t_2^{n/2} + \frac{n}{2}\, t_1^2\, t_2^{n/2-1}\right)$$

et la valeur de Z_{C_n} calculée précédemment fournit le résultat.

Passons maintenant aux polyèdres réguliers. On utilisera sans cesse le fait que leur groupe de rotations agissent transitivement sur l'ensemble de leurs sommets (c'est-à-dire que cette action possède une seule orbite).

- **Cas du tétraèdre.** Notons S_t le sous-groupe de $\mathrm{SO}(3,\mathbb{R})$ conservant le tétraèdre régulier, agissant sur l'ensemble X des sommets du tétraèdre. Le stabilisateur d'un sommet est cyclique d'ordre 3, et l'orbite est de cardinal 4 : l'action est transitive. Donc $|S_t| = 3 \cdot 4 = 12$. On peut maintenant lister les éléments de S_t, qui sont :
  - L'identité, qui a comme indicatrice des cycles t_1^4.
  - Les rotations non triviales fixant un sommet : il y en a $4 \cdot 2 = 8$, dont les indicatrice des cycles sont $t_1\, t_3$.
  - Les rotations non triviales fixant deux milieux d'arêtes opposés : il y en a trois, chacune d'indicatrice des cycles t_2^2.

Ce sont les seuls, car il y en a 12. Par conséquent

$$Z_{S_t} = \frac{1}{12}(t_1^4 + 8\, t_1\, t_3 + 3\, t_2^2).$$

- **Cas de l'octaèdre.** Notons S_o son groupe de symétries. Comme ci-dessus, le stabilisateur d'un sommet est cyclique d'ordre 4, donc $|S_o| = 4 \cdot 6 = 24$. Les éléments de S_o sont :
  - L'identité, d'indicatrice des cycles t_1^6.
  - Les rotations non triviales fixant une paire de sommets opposés : il y en a $3 \cdot 2 = 6$ d'angle $\pm\frac{\pi}{2}$, d'indicatrice des cycles $t_1^2\, t_4$, et trois d'angle π, d'indicatrice des cycles $t_1^2\, t_2^2$.
  - Les rotations non triviales fixant une paire de milieux d'arêtes opposés : il y en a six, d'indicatrice de cycle t_2^3.
  - Les rotations non triviales fixant une paire de centres de faces opposés : il y en a $4 \cdot 2 = 8$, d'indicatrice des cycles t_3^2.

Encore une fois, ce sont les seuls. On en déduit donc que

$$Z_{S_o} = \frac{1}{24}(t_1^4 + 6\, t_1^2\, t_4 + 3\, t_1^2\, t_2^2 + 6\, t_2^3 + 8 t_3^2).$$

- **Cas du cube.** Notons S_c le groupe des rotations du cube, qui est de cardinal $3 \cdot 8 = 24$. Les éléments en sont [3]
  - L'identité, d'indicatrice des cycles t_1^8.

3. Par dualité, on a en fait déjà la liste de ces éléments...

– Les rotations non triviales fixant une paire de sommets opposés : il y en a $4 \cdot 2 = 8$ d'ordre trois, d'indicatrice des cycles $t_1^2\, t_3^2$.
– Les rotations non triviales fixant une paire de milieux d'arêtes opposés : il y en a six, d'indicatrice des cycles t_2^4.
– Les rotations non triviales fixant une paire de centres opposés : il y en a $3 \cdot 2 = 6$ d'angle $\pm\frac{\pi}{2}$, d'indicatrice des cycles t_4^2, et trois d'angle π, d'indicatrice des cycles t_2^4.

On en conclut que

$$Z_{S_c} = \tfrac{1}{24}(t_1^8 + 8\, t_1^2\, t_3^2 + 9\, t_2^4 + 6\, t_4^2).$$

• **Cas de l'icosaèdre.** Notons S_i le groupe des rotations de l'icosaèdre. Il a $5 \cdot 12 = 60$ éléments, qui sont

– L'identité, d'indicatrice des cycles t_1^{12}.
– Les rotations non triviales fixant deux sommets opposés : il y en a $6 \cdot 4 = 24$, toutes d'ordre cinq, d'indicatrice des cycles $t_1^2\, t_5^2$.
– Les rotations non triviales fixant deux milieux d'arêtes opposés : il y en a 15, d'indicatrice des cycles t_2^6.
– Les rotations non triviales fixant deux centres de faces opposés : il y en a $10 \cdot 2 = 20$, d'indicatrice des cycles t_3^4.

On en déduit que

$$Z_{S_i} = \tfrac{1}{60}(t_1^{12} + 24\, t_1^2\, t_5^2 + 15\, t_2^6 + 20\, t_3^4).$$

• **Cas du dodécaèdre.** Le groupe S_d est d'ordre $3 \cdot 20 = 60$, et ses éléments sont

– L'identité, d'indicatrice des cycles t_1^{20}.
– Les rotations non triviales autour d'un sommet, au nombre de $10 \cdot 2 = 20$, et d'indicatrice des cycles $t_1^2\, t_3^6$.
– Les rotations non triviales autour d'une arête, au nombre de 15 et d'indicatrice des cycles t_2^{10}.
– Les rotations non triviales autour d'une face, au nombre de $6 \cdot 4 = 24$ et d'indicatrice des cycles t_5^4.

Finalement

$$Z_{S_d} = \tfrac{1}{60}(t_1^{20} + 20\, t_1^2\, t_3^6 + 15\, t_2^{10} + 24\, t_5^4).$$

Le théorème est donc démontré. □

Exemples.
• Le nombre de coloriages à k couleurs des sommets du polygone régulier à n côtés distincts à rotation près vaut

$$\frac{1}{n} \sum_{d|n} \varphi(d)\, k^{n/d}.$$

Le théorème de Pólya permet le calcul rapide d'un nombre de coloriage, mais il donne également en un seul calcul tous les nombres de coloriages, ce que nous illustrons maintenant.

- Cherchons la série génératrice des types de coloriages à trois couleurs de l'ensemble des sommets du carré, distincts à rotation près.

$$\begin{aligned} Z_{C_4} &= \frac{1}{4}\sum_{d|4} \varphi(d)\, t_d^{4/d} \\ &= \tfrac{1}{4}(\varphi(1)\, t_1^{4/1} + \varphi(2)\, t_2^{4/2} + \varphi(4)\, t_4^{4/4}) \\ &= \tfrac{1}{4}(t_1^4 + t_2^2 + 2\, t_4). \end{aligned}$$

On applique le théorème de Pólya :

$$\begin{aligned} U_{\Gamma/C_4}(x_1,x_2,x_3) &= Z_{C_4}(\tau_1,\tau_2,\tau_3,\tau_4) \\ &= \tfrac{1}{4}(\tau_1^4 + \tau_2^2 + 2\,\tau_4) \\ &= \tfrac{1}{4}((x_1+x_2+x_3)^4 + (x_1^2+x_2^2+x_3^3)^2 + 2\,(x_1^4+x_2^4+x_3^4)) \\ &= \langle x_1^4\rangle + \langle x_1^3\, x_2\rangle + 3\,\langle x_1^2\, x_2\, x_3\rangle + 2\,\langle x_1^2\, x_2^2\rangle \end{aligned}$$

où l'on a posé, pour tout monôme m de $\mathbb{Z}[x_1,x_2,x_3]$, $\langle m\rangle = \sum_{\ell\in\mathfrak{S}_3\cdot m} \ell$.

Comme on le vérifie facilement à la main, il existe donc un unique coloriage n'utilisant que la couleur rouge (correspondant à x_1^4), un unique coloriage utilisant trois fois la couleur rouge et une fois la couleur jaune (correspondant à $x_1^3\, x_2$), et trois coloriages utilisant deux fois la couleur rouge, une fois la couleur jaune et une fois la couleur bleue (correspondant à $x_1^2\, x_2\, x_3$).

- Cherchons la série génératrice des types de coloriages essentiellement distincts à deux couleurs de l'ensemble des faces du dodécaèdre régulier. Le dual de ce solide [4] étant l'icosaèdre, colorier les faces du dodécaèdre revient à colorier les sommets de l'icosaèdre. On a vu que

$$Z_{S_i} = \tfrac{1}{60}(t_1^{12} + 24\, t_1^2\, t_5^2 + 15\, t_2^6 + 20\, t_3^4)$$

d'où l'on tire par un calcul informatisé

$$\begin{aligned} U_{\Gamma/S_i} =& Z_{S_i}(\tau_1,\tau_2,\tau_3,\tau_4,\tau_5) \\ =& \langle x_1^{12}\rangle + \langle x_1^{11}\, x_2\rangle + 3\,\langle x_1^{10}\, x_2^2\rangle + 5\,\langle x_1^9\, x_2^3\rangle \\ &+ 12\,\langle x_1^8\, x_2^4\rangle + 14\,\langle x_1^7\, x_2^5\rangle + 24\,\langle x_1^6\, x_2^6\rangle \end{aligned}$$

où cette fois-ci $\langle m\rangle$ désigne $\sum_{\ell\in\mathfrak{S}_2\cdot m} \ell$ pour $m\in\mathbb{Z}[x_1,x_2]$. Il y a donc par exemple cinq dodécaèdres différents avec neuf faces blanches et trois faces noires.

4. C'est-à-dire le polyèdre dont les sommets sont les centres des faces du dodécaèdre, et les arêtes sont celles qui relient deux sommets provenant de faces adjacentes.

2.2 Action d'un groupe linéaire sur une droite projective

On a vu que l'indicatrice des cycles d'une action de groupe aidait à la compréhension de la combinatoire de cette action. Dans ce paragraphe, nous étudions par cette méthode l'action du groupe linéaire des matrices de taille 2 sur la droite projective d'un corps fini.

Ici, q désignera une puissance différente de 1 d'un nombre premier p. On rappelle que l'ordre de $\mathrm{GL}_2(\mathbb{F}_q)$ est $(q^2-1)(q^2-q)$.

Théorème 6. *L'indicatrice des cycles pour l'action naturelle de* $\mathrm{GL}_2(\mathbb{F}_q)$ *sur la droite projective* $\mathbb{P}^1(\mathbb{F}_q)$ *vaut*

$$\frac{1}{(q-1)\,q\,(q+1)}\,t_1^{q+1} + \frac{1}{q}\,t_1\,t_p^{\frac{q}{p}} + \frac{1}{2\,(q-1)}\sum_{1\neq d\mid q-1}\varphi(d)\,t_1^2\,t_d^{\frac{q-1}{d}} + \frac{1}{2\,(q+1)}\sum_{1\neq d\mid q+1}\varphi(d)\,t_d^{\frac{q+1}{d}}.$$

La preuve du théorème se décompose en deux grandes étapes : on commence par décrire les classes de similitude de $\mathrm{GL}_2(\mathbb{F}_q)$, puis on détermine pour chacune de ces classes l'indicatrice des cycles associée — deux éléments d'une même classe agissant de façon semblable sur $\mathbb{P}^1(\mathbb{F}_q)$. On conclut en sommant les différentes contributions.

2.2.1 Classes de similitude de $\mathrm{GL}_2(\mathbb{F}_q)$

Proposition 7. *Les classes de similitude de* $\mathrm{GL}_2(\mathbb{F}_q)$ *sont de quatre types, résumés dans le tableau 2 ci-dessous, qui récapitule pour chaque classe la forme d'un représentant, le cardinal de la classe et le nombre de telles classes.*

Type	Représentant	Cardinal	Nombre
homothéties	$\left(\begin{smallmatrix}\alpha & \\ & \alpha\end{smallmatrix}\right)$	1	$q-1$
diagonalisables à valeurs propres distinctes	$\left(\begin{smallmatrix}\alpha & \\ & \beta\end{smallmatrix}\right)$	$q\,(q+1)$	$\dfrac{(q-1)\,(q-2)}{2}$
trigonalisables non diagonalisables	$\left(\begin{smallmatrix}\alpha & 1 \\ & \alpha\end{smallmatrix}\right)$	$(q-1)\,(q+1)$	$q-1$
non trigonalisables	$\left(\begin{smallmatrix}\lambda & \\ & \bar{\lambda}\end{smallmatrix}\right)$	$q\,(q-1)$	$\dfrac{q\,(q-1)}{2}$

TABLE 2 – Classes de similitude de $\mathrm{GL}_2(\mathbb{F}_q)$

Pour dénombrer les classes de similitudes, on utilisera les propriétés de l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ sur lui-même par conjugaison. En effet pour cette action, les

orbites sont exactement les classes de similitude. De plus le stabilisateur d'un élément $x \in \mathrm{GL}_2(\mathbb{F}_q)$ est son *centralisateur* : le sous-groupe des éléments qui commutent avec lui. Le cardinal de la classe de similitude de x est donc $\frac{(q^2-1)\,(q^2-q)}{c}$, où c est le cardinal de son centralisateur.

Démontrons la proposition 7. On considère le polynôme caractéristique d'une matrice de $\mathrm{GL}_2(\mathbb{F}_q)$. S'il admet deux racines distinctes dans $\mathbb{F}_q$, la matrice est diagonalisable à valeurs propres distinctes. S'il a deux racines identiques, soit la matrice est une homothétie, soit elle est trigonalisable non diagonalisable ; quitte à conjuguer par une dilatation, on se ramène à la forme ci-dessus. Enfin, si le polynôme caractéristique est irréductible, il est scindé à racines simples dans $\mathbb{F}_{q^2}$. Étudions séparément les différents cas.

- **Cas d'une homothétie.** Étant centrale, sa classe est réduite à un élément. Il y a exactement une classe par élément de $\mathbb{F}_q^\times$, ce qui donne $q-1$ classes.

- **Cas d'une matrice diagonalisable à valeurs propres distinctes.** Pour obtenir le cardinal de sa classe de similitude, calculons son centralisateur. Une matrice commutant avec elle laisse stables ses droites propres, et est donc diagonale dans la même base ; réciproquement, toutes les matrices de ce type sont dans le centralisateur. Il est donc de cardinal $(q-1)^2$, d'où le cardinal de l'orbite sous l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ par conjugaison. Par ailleurs, il y a exactement une classe par partie à deux éléments de $\mathbb{F}_q^\times$, soit $\binom{q-1}{2} = \frac{(q-1)\,(q-2)}{2}$.

- **Cas d'une matrice trigonalisable non diagonalisable.** Comme précédemment, on calcule son centralisateur. On trouve qu'il s'agit des matrices triangulaires supérieures dans la même base, de valeurs propres identiques. Il est donc de cardinal $q\,(q-1)$, et l'orbite a bien le cardinal annoncé. Et il y a autant de classes que de valeurs propres possibles, soit $q-1$.

- **Cas d'une matrice non trigonalisable.** après conjugaison par une matrice de $\mathrm{GL}_2(\mathbb{F}_{q^2})$, elle s'écrit $\left(\begin{smallmatrix}\lambda & \\ & \bar\lambda\end{smallmatrix}\right)$ où $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ et où $\bar\lambda$ est l'autre racine du polynôme caractéristique. On calcule encore une fois le centralisateur de cette matrice : un élément de ce centralisateur se diagonalise dans la même base en $\left(\begin{smallmatrix}\alpha & \\ & \beta\end{smallmatrix}\right)$, et un tel élément provient du centralisateur dans $\mathrm{GL}_2(\mathbb{F}_q)$ si et seulement si $\beta = \bar\alpha$; en effet, la condition est nécessaire en considérant le spectre, et elle est suffisante par le lemme 8 ci-après. Il y en a donc exactement un par élément de $\mathbb{F}_{q^2}^\times$, soit q^2-1, et l'orbite est de cardinal $q\,(q-1)$. Enfin, il y a exactement une classe de similitude par paire de conjugués $\{\lambda, \bar\lambda\}$ avec $\lambda \notin \mathbb{F}_q$, soit $\frac{q^2-q}{2}$. □

On s'est servi du lemme technique que voici :

Lemme 8. *Soit $g = P\left(\begin{smallmatrix}\lambda & \\ & \bar\lambda\end{smallmatrix}\right)P^{-1} \in \mathrm{GL}_2(\mathbb{F}_q)$ avec $P \in \mathrm{GL}_2(\mathbb{F}_{q^2})$ et $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. alors, pour tout $\mu \in \mathbb{F}_{q^2}^\times$, la matrice $P\left(\begin{smallmatrix}\mu & \\ & \bar\mu\end{smallmatrix}\right)P^{-1}$ appartient à $\mathrm{GL}_2(\mathbb{F}_q)$.*

Démonstration. Considérons l'application $\mathbb{F}_q$-linéaire

$$\begin{array}{rccc} f: & \mathbb{F}_{q^2} & \longrightarrow & \mathcal{M}_2(\mathbb{F}_{q^2}) \\ & \mu & \longmapsto & P\begin{pmatrix}\mu & \\ & \bar{\mu}\end{pmatrix}P^{-1}. \end{array}$$

Elle est injective et son image est donc de dimension 2 sur $\mathbb{F}_q$. Or cette image contient $f(1) = 1 \in \mathcal{M}_2(\mathbb{F}_q)$ et $f(\lambda) = g \in \mathcal{M}_2(\mathbb{F}_q)$ qui n'est pas une homothétie : comme $\lambda \notin \mathbb{F}_q$, c'est que $\lambda \neq \bar{\lambda}$. Par conséquent, $f(1)$ et $f(\lambda)$ sont indépendants sur $\mathbb{F}_q$, et donc engendrent l'image de f qui est finalement incluse dans $\mathcal{M}_2(\mathbb{F}_q)$. □

2.2.2 Calcul des indicatrices des cycles

Nous sommes maintenant en mesure de prouver le théorème 6. Comme les éléments de $\mathrm{GL}_2(\mathbb{F}_q)$ induisent des permutations de $\mathbb{P}^1(\mathbb{F}_q)$, les indicatrices de cycles ne dépendent que de la classe de similitude d'un élément ; il nous suffit donc de calculer l'indicatrice des cycles des quatre types de représentants listés ci-dessus.

- **Cas d'une homothétie.** Les homothéties agissent trivialement sur $\mathbb{P}^1(\mathbb{F}_q)$, et ont donc chacune pour indicatrice des cycles t_1^{q+1}. La somme de ces indicatrices est donc $(q-1)\,t_1^{q+1}$.

- **Cas d'une matrice diagonalisable à valeurs propres distinctes.** La matrice $g = \left(\begin{smallmatrix}\alpha & \\ & \beta\end{smallmatrix}\right)$ est proportionnelle à $\left(\begin{smallmatrix}\alpha\,\beta^{-1} & \\ & 1\end{smallmatrix}\right)$, qui agit sur la droite projective $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q^\times \sqcup \{0\} \sqcup \{\infty\}$ par multiplication par $\alpha\,\beta^{-1}$. Son indicatrice des cycles est donc

$$\zeta_g = t_1^2\, t_d^{\frac{q-1}{d}}$$

où $d = \mathrm{ord}(\alpha\,\beta^{-1})$ désigne l'ordre multiplicatif de $\alpha\,\beta^{-1}$ dans $\mathbb{F}_q^\times$. En sommant les indicatrices de cycles de toutes les classes et en les regroupant par ordre, on obtient

$$\begin{aligned} \frac{1}{2}\sum_{\alpha\neq\beta\in\mathbb{F}_q^\times} q\,(q+1)\,t_1^2\,t_{\mathrm{ord}(\alpha\,\beta^{-1})}^{\frac{q-1}{\mathrm{ord}(\alpha\,\beta^{-1})}} &= \frac{q\,(q+1)}{2}\sum_{\gamma\in\mathbb{F}_q^\times\setminus\{1\}}\ \sum_{\beta\in\mathbb{F}_q^\times} t_1^2\,t_{\mathrm{ord}\,\gamma}^{\frac{q-1}{\mathrm{ord}\,\gamma}} \quad (\gamma = \alpha\,\beta^{-1}) \\ &= \frac{(q-1)\,q\,(q+1)}{2}\sum_{\gamma\in\mathbb{F}_q^\times\setminus\{1\}} t_1^2\,t_{\mathrm{ord}\,\gamma}^{\frac{q-1}{\mathrm{ord}\,\gamma}} \\ &= \frac{(q-1)\,q\,(q+1)}{2}\sum_{1\neq d\mid q-1}\varphi(d)\,t_1^2\,t_d^{\frac{q-1}{d}} \end{aligned}$$

car $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, et a donc exactement $\varphi(d)$ éléments d'ordre d pour tout diviseur d de $q-1$.

- **Cas d'une matrice trigonalisable non diagonalisable.** La matrice diagonale $\left(\begin{smallmatrix}\alpha & 1\\ & \alpha\end{smallmatrix}\right)$ est proportionnelle à $\left(\begin{smallmatrix}1 & \alpha^{-1}\\ & 1\end{smallmatrix}\right)$, elle-même semblable à $\left(\begin{smallmatrix}1 & 1\\ & 1\end{smallmatrix}\right)$. Toutes les matrices de ces classes de similitude agissent donc sur $\mathbb{P}^1(\mathbb{F}_q)$ comme cette dernière, qui est une translation additive sur $\{\infty\} \sqcup \mathbb{F}_q$. Leurs indicatrices de cycles sont donc toutes $t_1\, t_p^{q/p}$, puisque l'ordre de 1 dans le groupe additif $\mathbb{F}_q$ est p. En sommant, on obtient

$$(q-1)^2\,(q+1)\,t_1\,t_p^{q/p}.$$

- **Cas d'une matrice non trigonalisable.** Soit $g = P\left(\begin{smallmatrix}\lambda & \\ & \bar{\lambda}\end{smallmatrix}\right)P^{-1}$ une telle matrice, avec $P \in \mathrm{GL}_2(\mathbb{F}_{q^2})$ et $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. D'après le lemme 8, on a un morphisme de groupes

$$\begin{array}{ccc} \mathbb{F}_{q^2}^\times & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_q) \\ \mu & \longmapsto & P\begin{pmatrix}\mu & \\ & \bar{\mu}\end{pmatrix}P^{-1} \end{array}$$

qui induit une action de $\mathbb{F}_{q^2}^\times$ sur $\mathbb{P}^1(\mathbb{F}_q)$, dans laquelle λ agit comme g. Le noyau de cette action est la préimage de l'ensemble des homothéties, soit exactement $\mathbb{F}_q^\times$, et on a par conséquent une action de $\mathbb{T}_q = \mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times$ sur $\mathbb{P}^1(\mathbb{F}_q)$, pour laquelle la classe $[\lambda]$ de λ agit comme g. Cette action est simple : en effet, si un élément $[\lambda]$ de $\mathbb{T}_q$ a un point fixe, alors l'image de λ a une droite stable, et donc une valeur propre dans $\mathbb{F}_q$, et $\lambda \in \mathbb{F}_q$, soit $[\lambda] = 1$. En choisissant un élément quelconque D de $\mathbb{P}^1(\mathbb{F}_q)$, on a donc une injection de $\mathbb{T}_q$ dans $\mathbb{P}_1(\mathbb{F}_q)$ donnée par $\gamma \mapsto \gamma \cdot D$, qui est une bijection par égalité des cardinaux. Finalement, l'action de $\mathbb{T}_q$ sur $\mathbb{P}_1(\mathbb{F}_q)$ s'identifie à l'action de $\mathbb{T}_q$ sur lui-même par multiplication.

Par conséquent,

$$\zeta_g = \zeta_\lambda = \zeta_{[\lambda]} = t_{\mathrm{ord}[\lambda]}^{\frac{q+1}{\mathrm{ord}[\lambda]}}$$

où ord désigne cette fois-ci l'ordre multiplicatif dans le groupe $\mathbb{T}_q$. En sommant sur toutes les classes, on obtient

$$\begin{aligned} \frac{1}{2}\sum_{\lambda\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} q\,(q-1)\,t_{\mathrm{ord}[\lambda]}^{\frac{q+1}{\mathrm{ord}[\lambda]}} &= \frac{q\,(q-1)}{2}\sum_{\gamma\in\mathbb{T}_q\setminus\{1\}} (q-1)\,t_{\mathrm{ord}\,\gamma}^{\frac{q+1}{\mathrm{ord}\,\gamma}} \\ &= \frac{q\,(q-1)^2}{2}\sum_{1\neq d\mid q+1} \varphi(d)\,t_d^{\frac{q+1}{d}} \end{aligned}$$

puisque $\mathbb{T}_q$ est cyclique d'ordre $q+1$ comme quotient du groupe cyclique $\mathbb{F}_{q^2}^\times$. Il suffit enfin de sommer les différentes contributions pour aboutir à la formule annoncée. □

Remarque. Il n'est en fait pas surprenant d'avoir une bijection entre $\mathbb{T}_q$ et la droite projective $\mathbb{P}^1(\mathbb{F}_q)$, puisque $\mathbb{F}_{q^2}$ est (non canoniquement) isomorphe à $\mathbb{F}_q^2$ en tant que $\mathbb{F}_q$-espace vectoriel, ce qui induit une bijection entre $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times$ et $(\mathbb{F}_q^2 \setminus \{0\})/(\mathbb{F}_q^\times)$.

Références

[Aud06] Audin, Michèle: *Géométrie*. EDP Sciences, 2006.

[Big89] Biggs, Norman L.: *Discrete mathematics*. Oxford Science Publications. New York, deuxième édition, 1989.

[Cal84] Calais, Josette: *Eléments de théorie des groupes*. Presses universitaires de France, Paris, 1984.

[Dem97] Demazure, Michel: *Cours d'algèbre*. Nouvelle bibliothèque mathématique. Cassini, Paris, 1997.

[Per82] Perrin, Daniel: *Cours d'algèbre*. École normale supérieure de jeunes filles, Paris, 1982.

[Sam86] Samuel, Pierre: *Géométrie projective*. Presses universitaires de France, Paris, 1986.