Un jeu de taquin pour le groupe de Mathieu M_{12}

Théo BIGOTTE, sous la direction de Jérôme GERMONI

27 juin 2024

Table des matières

Introduction

Le groupe de Mathieu M_{12} est un groupe fini simple de cardinal 95 040. Il est très liés à des objets combinatoires assez différents : le système de Steiner $S(5,6,12)$, sur lequel il agit et qui est même son groupe d'automorphismes ; le code de Golay ternaire étendu, qui est « presque » son groupe d'automorphismes (c'est-à-dire qu'une extension double de M_{12}) ; les matrices d'Hadamard 12×12.

Une construction due à Conway et développée par Conway, Elkies et Martin dans [1] permet de retrouver tous ces objets et toutes ces actions de façon naturelle (i.e. sans choix, ou alors en contrôlant parfaitement l'effet de ces choix), à partir d'une structure combinatoire très simple : le plan projectif sur le corps à trois éléments. C'est beaucoup plus convaincant que la construction habituelle où les générateurs de M_{12} sont parachutés ou d'autres par extensions successives de systèmes de Steiner plus petits – cf. [2].

Dans ce texte, après quelques rappels sur les notions de plan projectif, et introduction aux systèmes de Steiner. On va décrire une réalisation explicite du groupe de Mathieu M_{12} et du groupe des automorphismes du code de Golay ternaire étendu à partir du plan projectif sur $\mathbb{F}_3$. On admet (de façon provisoire) l'existence et (de façon définitive) l'unicité d'un système de Steiner $S(5,6,12)$. Cela donne un sens à la définition de M_{12} comme groupe d'automorphisme « du » $S(5,6,12)$.

On part du $S(2,4,13)$ qu'est le plan projectif fini $\mathscr{P} = \mathbb{P}^2(\mathbb{F}_3)$: il permet de définir :

— un code $\mathscr{C}$ dans $\mathbb{F}_3^{13}$;

— des sous-codes $\mathscr{C}_p$ dans $\mathscr{C}$ et $\mathscr{G}_p$ dans $\mathbb{F}_3^{12}$ (pour $p \in \mathscr{P}$).

En implémentant ces objets, on vérifie que chaque $\mathscr{G}_p$ est isomorphe au code de Golay ternaire étendu. L'ensemble W_6 des supports des vecteurs de poids 6 forme un $S(5,6,12)$. Avec un $S(5,6,12)$ sous la main, on détermine son groupe d'automorphismes : on donne un algorithme qui, pour chaque couple de quintuplets ordonnés de points distincts (x,y), renvoie un automorphisme qui envoie x_i sur y_i pour $0 \leq i \leq 4$ sous réserve qu'il en existe un. Le fait que l'algorithme aboutisse pour x fixé et tous les y montre qu'il y a autant d'automorphismes que de quintuplets, i.e. 95 040 et que les groupe d'automorphismes est cinq fois simplement (*sharply*) transitif.

Les objets précédents admettent des symétries définies aussi grâce au plan projectif $\mathscr{P}$: à chaque chemin fermé de $\mathscr{P}$ (suite finie de points dont le premier et le dernier sont un élément fixé noté 0), on associe :

— une permutation de 12 points ; toutes ces permutations forment un groupe appelé « groupe du jeu de base » et noté G_{bas} ;

— une matrice monomiale 12×12 ; toutes ces matrices monomiales forment un groupe appelé « groupe du jeu signé » et noté G_{sgn}.

On a en plus, par construction, un morphisme surjectif de G_{sgn} sur G_{bas}, restriction du morphisme évident des matrices monomiales sur les (matrices de) permutations. Une implémentation de ces transformations permet de voir que G_{bas} contient au moins 95 040 éléments et G_{sgn} au moins le double. On montre que G_{sgn} agit sur $\mathscr{G}_0$ (l'un des $\mathscr{G}_p$) par automorphismes. Il en résulte que G_{bas} agit sur $S(5,6,12)$ par automorphismes, puis que G_{bas} est isomorphe à M_{12}. De plus le noyau de la projection $\mathrm{Aut}\,\mathscr{G}_0 \to \mathrm{Aut}\,\mathrm{W}_6$ est d'ordre 2, comme celui de $G_{sgn} \to G_{bas}$. Pour des raisons de cardinal, on obtient alors que G_{sgn} est isomorphe au groupe des automorphismes du code de Golay et que son quotient par un groupe d'ordre 2 est isomorphe au groupe de Mathieu M_{12}. En poursuivant un peu, on a vu mais pas écrit qu'une variante du jeu basique prenant en compte l'espace projectif dual de $\mathbb{P}^2(\mathbb{F}_3)$ permet de :

— réaliser un automorphisme extérieur de M_{12} ;

— réaliser M_{12} comme groupe des automorphismes d'une matrice d'Hadamard 12×12.

1 Systèmes de Steiner et plans projectifs

Références : [1], [2], [4], [5].

1.1 Définitions

1.1.1 Système de Steiner

Débutons cette partie par une définition.

Définition (système de Steiner $S(r,k,n)$)**.** Soient r, k, n trois entiers tels que $0 < r < k < n$. On appelle système de Steiner, noté $S(r,k,n)$, sur I un ensemble à n éléments, la donnée d'un ensemble S de parties de I, qui ont toutes k éléments et vérifiant la propriété :

toute partie à r éléments de I est contenue dans un unique élément de S.

Exemple. Considérons l'ensemble $I = \{1, \dots, 7\}$ et

$$S = \{\{2,4,6\},\{1,4,5\},\{3,7,4\},\{1,2,3\},\{2,7,5\},\{1,7,6\},\{3,6,5\}\}.$$

Pour la prochaine figure, on réécrit $S = \{\overline{1}, \dots, \overline{7}\}$. Vérifions qu'il s'agit d'un système de Steiner $S(2,3,7)$. Tout d'abord, on a $n = |I| = 7$, on voit que l'ensemble S est constitué de parties à $k = 3$ éléments. Montrons donc que tout couple ($r = 2$) de I est contenu dans un unique triplet de S. La vérification est immédiate et on peut résumer les résultats dans le tableau suivant.

Couple $\{i,j\}$ de I	Droite	Numéro
$\{2,4\}$, $\{4,6\}$, $\{2,6\}$	$\{2,4,6\}$	$\overline{1}$
$\{1,4\}$, $\{1,5\}$, $\{4,5\}$	$\{1,4,5\}$	$\overline{2}$
$\{3,7\}$, $\{3,4\}$, $\{7,4\}$	$\{3,7,4\}$	$\overline{3}$
$\{1,2\}$, $\{1,3\}$, $\{2,3\}$	$\{1,2,3\}$	$\overline{4}$
$\{2,7\}$, $\{2,5\}$, $\{7,5\}$	$\{2,7,5\}$	$\overline{5}$
$\{1,7\}$, $\{1,6\}$, $\{7,6\}$	$\{1,7,6\}$	$\overline{6}$
$\{3,6\}$, $\{3,5\}$, $\{5,6\}$	$\{3,6,5\}$	$\overline{7}$

TABLE 1 – Tableau de correspondance entre couples et droites

On peut à partir de ce tableau construire une représentation du plan de Fano (voir la figure 1).

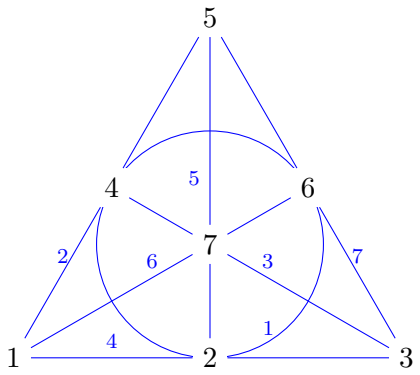

FIGURE 1 – Plan de Fano

Les systèmes de Steiner sont également associés au *triangle d'intersection*, structure présentée dans l'article [5]. Soit $S(r,k,n)$ un système de Steiner. Le triangle est une famille d'entiers $(t_{i,j})_{0 \le j \le i \le r}$. Si $\{x_1, \dots, x_k\}$ est un bloc, le j-ème coefficient de la i-ème ligne est le nombre de blocs qui contiennent $x_1, \dots, x_j$ mais pas $x_{j+1}, \dots, x_i$.

Lemme. *Le triangle d'intersection vérifie les propriétés suivantes :*

1. $t_{i,i} = \frac{\binom{n-i}{r-i}}{\binom{k-i}{r-i}} si\ i \geq 1$;
2. $t_{i,j} = t_{(i+1,j)} + t_{(i+1,j+1)}$.

Démonstration. Soit $S(r,k,n)$ un système de Steiner.

— On suppose d'abord $i \leq r$. À toute partie A à $r-i$ éléments de $I \setminus \{x_1, \ldots, x_i\}$, on associe l'unique bloc qui contient $\{x_1, \ldots, x_i\} \cup A$. Un bloc contenant $\{x_1, \ldots, x_i\}$ admet autant d'antécédents que de façons de choisir A dans le bloc, c'est-à-dire de choisir $r-i$ éléments parmi les $k-i$ éléments du bloc autres que $x_1, \ldots, x_i$. D'après le lemme des bergers, le nombre de blocs contenant $\{x_1, \ldots, x_i\}$ est donc $t_{i,i} = \binom{n-i}{r-i}/\binom{k-i}{r-i}$.

— Si $r \leq i$, l'unique bloc contenant $\{x_1, \ldots, x_i\}$ est simplement l'unique bloc contenant $\{x_1, \ldots, x_r\}$ car on sait a priori que $\{x_1, \ldots, x_i\}$ est contenu dans un bloc. Autrement dit, $t_{i,i} = 1$.

Le deuxième point se démontre par récurrence grâce aux coefficients $t_{i-1,i-1}$ et $t_{i,i}$ qui vérifie pour tout i la relation de Pascal, nous le voyons directement sur les tables suivantes. □

Exemple. Pour $S(5,6,12)$, lorsqu'on se donne la donnée de quatre points $x_1, \cdots, x_4$, on doit en choisir un autre point parmi les huit restants $\binom{8}{1}$ pour obtenir un quintuplet, qui est par propriété du $S(5,6,12)$ inclus dans un unique bloc. Et se donner un cinquième point x_5, c'est en imposer un sixième x_6. Mais le choix de ce cinquième aurait pu être le sixième dès le départ. On a en fait les blocs $\{x_1, \cdots, x_4, x_5, x_6\}$ ou $\{x_1, \cdots, x_4, x_6, x_5\}$ qui comprenent notre quadruplet de départ. Il y'a deux choix $\binom{2}{1}$ possibles donc. Ce qui amène le nombre de bloc pour un quadruplet donné $t_{4,4} = \binom{8}{1}\backslash\binom{2}{1} = 4$.

Corollaire. *Le triangle d'un $S(2,3,7)$ est la table 2.*

			7			
		4		3		
	2		2		1	
0		2		0		1

TABLE 2 – Triangle d'intersection du $S(2,3,7)$

Corollaire. *Le triangle d'un $S(5,6,12)$ est la table 3.*

					132						
				66			66				
			30			66			30		
		12			18			18			12	
	4			8			10			8			4	
1			3			5			5			3			1
1		0			3			2			3			0		1

TABLE 3 – Triangle d'intersection du $S(5,6,12)$

Remarque. Pour $S(5,6,12)$, nous lisons le coefficient le plus en bas à droite, $t_{6,6}$ que pour un bloc $\{x_1, \ldots, x_6\}$, il y a 1 bloc qui contient qui contient $x_1, \ldots, x_j = x_6$, c'est lui même. Le nombre $t_{5,5}$ nous dit qu'un quintuplet est contenu dans un unique bloc.

Corollaire. *Dans un $S(5,6,12)$, le complémentaire d'un bloc est un bloc.*

Démonstration. Dans $S(5,6,12)$, le coefficient le plus en bas à gauche $t_{6,0}$, nous montre qu'il y a un bloc qui ne contient pas $x_1, \ldots, x_6$, c'est en fait le complémentaire. □

1.1.2 Plans projectifs finis

Définition (plan projectif). Soit $\mathscr{P}$ un ensemble fini d'éléments appelés « points », et soit $\mathscr{L}$ une famille de parties de $\mathscr{P}$ appelées « droites ». Pour p dans $\mathscr{P}$, notons $\mathscr{L}(p)$ l'ensemble des éléments de $\mathscr{L}$ qui contiennent le point p. On dit que $(\mathscr{P}, \mathscr{L})$ est un plan projectif d'ordre n si :

1. $|\mathscr{P}| = |\mathscr{L}| = n^2 + n + 1$;
2. $|\mathscr{L}(p)| = |l| = n + 1$ pour $p \in \mathscr{P}$ et $l \in \mathscr{L}$;
3. deux points distincts $p, q \in \mathscr{P}$ appartiennent à une et une seule droite ;
4. deux droites distinctes $l, m \in \mathscr{L}$ s'intersectent en un seul et unique point ;
5. il existe au moins quatre points trois à trois non alignés.

Afin de mieux comprendre et appréhender la notion de système de Steiner, vérifions que les plans projectifs en sont un exemple.

Proposition. *La donnée d'un plan projectif équivaut à la donnée d'un $S(2, n+1, n^2+n+1)$. En particulier, tout $S(2, n+1, n^2+n+1)$ est « autodual ».*

Démonstration. La définition du plan projectif $(\mathscr{P}, \mathscr{L})$ permet l'identification à deux systèmes de Steiner. En effet, l'ensemble $\mathscr{P}$ et $\mathscr{L}$ sont tous deux de cardinal n^2+n+1 ; chaque droite est constituée de $n+1$ points, chaque point appartient à $n+1$ droites. Et on précise ensuite que deux points sont contenus dans une unique droite ; respectivement deux droites s'intersectent en un et unique point. Le plan projectif donne ainsi lieu a deux systèmes de Steiner. On peut formaliser ceci : on a d'un côté $I_1 = \mathscr{P}$ et $S_1 = \mathscr{L}$ forment bien un $S(2, n+1, n^2+n+1)$. De l'autre, on définit $I_2 = \mathscr{L}$ et $S_2 = \{\mathscr{L}(p) : p \in \mathscr{P}\}$. Pour $k = 1$ puis $k = 2$, S_k est bien un ensemble des parties de I_k à $n+1$ éléments et toute partie à deux éléments de I_k est contenue dans un unique élément de S_k.

Ce résultat reflète en fait la notion de dualité en géometrie projective comme on le verra dans la partie 1.1.3. □

Remarque. Il est assez clair que le $S(2, 3, 7)$ présenté plus tôt définit un plan projectif fini d'ordre 2.

Proposition. *Tout système de Steiner $S(2, n+1, n^2+n+1)$ donne lieu à un plan projectif. Autrement dit :*

1. *il y a exactement n^2+n+1 droites ;*
2. *par chaque point passent exactement $n+1$ droites ;*
3. *deux droites quelconques ont exactement un point commun.*

Démonstration. Soit $(\mathscr{P}, S)$ un système de Steiner $S(2, n+1, n^2+n+1)$.

À toute paire $\{p_1, p_2\}$, on associe l'unique bloc qui la contient : par propriété des systèmes de Steiner. On obtient une application par laquelle chaque bloc admet $\binom{n+1}{2}$ antécédents (car chaque bloc contient $n+1$ points). Comme il y a $\binom{n^2+n+1}{2}$ paires de points, le lemme des bergers permet de calculer le nombre de blocs :

$$\frac{\binom{n^2+n+1}{2}}{\binom{n+1}{2}} = \frac{\frac{(n^2+n+1)(n^2+n)}{2}}{\frac{(n+1)n}{2}} = n^2+n+1.$$

Soit p_0 un point de $\mathscr{P}$. Soit $S(p_0)$ l'ensemble des blocs contenant p_0. À tout point p de $\mathscr{P} \setminus \{p_0\}$ on associe l'unique bloc contenant $\{p_0, p\}$. Chaque élément de $S(p_0)$ admet exactement n antécédent, d'où par le lemme des bergers :

$$\big|S(p_0)\big| = \frac{n^2+n+1-1}{n} = n+1.$$

Considérons l'ensemble PB des paires de blocs $\{l_1, l_2\}$ et l'ensemble PB_s formé des paires sécantes, i.e. les paires $\{l_1, l_2\}$ tel que $l_1 \cap l_2$ n'est pas vide – l'intersection est alors un singleton. On définit une application de PB_s vers $\mathscr{P}$: à la paire sécante $\{l_1, l_2\}$ on associe le point d'intersection l_1 et l_2.

Comme chaque point appartient à $n+1$ droites, chaque point admet $\binom{n+1}{2}$ antécédents. Il y a donc $\binom{n+1}{2}(n^2+n+1)$ paires sécantes. Par ailleurs le nombre de paires est [1]

$$\binom{n^2+n+1}{2} = \frac{(n^2+n+1)(n^2+n)}{2} = \binom{n+1}{2}(n^2+n+1).$$

Autrement dit, toute paire est une paire sécante, ce qui termine la démonstration. □

1.1.3 Plans projectifs sur un corps fini

Voici quelques rappels sur les corps finis. Ainsi, on sait que pour tout q puissance d'un nombre premier, il existe un corps de cardinal q, unique à isomorphisme près, noté $\mathbb{F}_q$, et que tout corps fini est isomorphe à un $\mathbb{F}_q$ (voir [2], page 222).

Proposition. *Soit q une puissance d'un nombre premier, et $\mathbb{F}_q$ le corps fini de cardinal q. À $\mathbb{F}_q$ est associé à un plan projectif et donc un système de Steiner $S(2, q+1, q^2+q+1)$: les points sont les droites vectorielles de $\mathbb{F}_q^3$ et les droites « sont » des plans vectoriels de $\mathbb{F}_q^3$.*

Nous proposons à la suite de ce paragraphe deux exemples de visualisation pour $q = 2$ et $q = 3$ (voir figure 2). On peut par ailleurs constater que le cas $q = 2$ donne lieu au système de Steiner présenté dans la partie 1.1.1. Dans la figure pour $q = 2$, on note $x_1x_2x_3$ la droite engendrée par $(x_1, x_2, x_3) \in \mathbb{F}_2^3 \setminus \{(0,0,0)\}$. La construction est « réalisée » par une équation. En effet, pour p et q deux points, le troisième point de la droite (pq) est $p+q$ qui est la seule combinaison linéaire non triviale de p et q dans $\mathrm{Vect}(p, q)$.

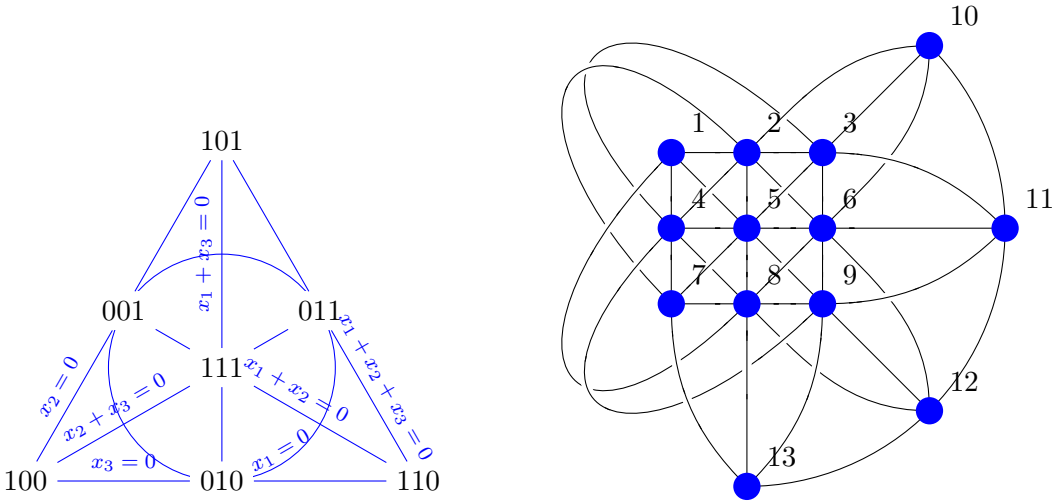

FIGURE 2 – Représentation des espaces projectifs $\mathbb{P}^2(\mathbb{F}_2)$ et $\mathbb{P}^2(\mathbb{F}_3)$

1.2 Automorphismes d'un système de Steiner

Maintenant que la notion de système de Steiner est présentée, étudions-en les automorphismes.

Définition (automorphisme)**.** On appelle automorphisme d'un système de Steiner (I, S) une bijection de I dans I qui induit [2] une bijection de S dans S.

Il est également utile pour la suite de voir la définition suivante.

1. NB : c'est la même égalité que la première formule centrée de la démonstration.
2. Rappelons que si $\sigma : I \longrightarrow I$ est une bijection, alors σ induit une bijection notée σ_* ou, par abus, σ, de l'ensemble $\mathscr{P}(I)$ des parties de I dans lui-même, définie par $\sigma_*(J) = \{\sigma(j) : j \in J\}$ pour $J \subset I$.

Définition (équivalence de deux système de Steiner)**.** Soit $S(k, r, n)$ un système de Steiner. Soient (I, S) et (I', S') où $S \subset \mathscr{P}_r(i)$, $S' \subset \mathscr{P}'_r(I')$. On appelle équivalence de deux systèmes de Steiner toute bijection $f : I \longrightarrow I'$ qui induit une bijection de S sur S'.

Reprenons l'exemple vu plus tôt, le plan du Fano.

Exemple. Les « symétries axiales » donnent les premiers exemples d'automorphismes. Nous constatons que la symétrie par rapport à la « médiatrice » $(1, 7, 6)$ conserve la structure d'incidence. En effet, changer le point 4 avec le point 2 et changer le point 5 avec le point 3 stabilise les droites. De même, les symétries par rapport aux « médiatrices » $(5, 7, 2)$ et $(3, 7, 4)$ sont des automorphismes.

Exemple. On trouve un autre exemple d'automorphisme d'ordre sept en identifiant $\mathbb{F}_2^3$ avec le corps $\mathbb{F}_8$. On réalise $\mathbb{F}_8$ comme $\mathbb{F}_2[X]/(X^3 + X + 1)$. C'est à dire que, $\mathbb{F}_8$ est engendré par un élément β vérifiant $\beta^3 = \beta + 1$ et $(1, \beta, \beta^2)$ est une base de $\mathbb{F}_8$ comme un $\mathbb{F}_2$-espace vectoriel. On écrit dans le tableau suivant les éléments de ce corps.

Élément	Égalité	Point
$1 = \beta^7$	$1 = 1$	$(1, 0, 0)$
β	$\beta = \beta$	$(0, 1, 0)$
β^2	$\beta^2 = \beta^2$	$(0, 0, 1)$
β^3	$\beta^3 = 1 + \beta$	$(1, 1, 0)$
β^4	$\beta^4 = \beta^3 \times \beta = \beta + \beta^2$	$(0, 1, 1)$
β^5	$\beta^5 = \beta^4 \times \beta = 1 + \beta + \beta^2$	$(1, 1, 1)$
β^6	$\beta^6 = \beta^5 \times \beta = 1 + \beta^2$	$(1, 0, 1)$

TABLE 4 – Correspondance entre éléments de $\mathbb{F}_8$ et points de $\mathbb{F}_2^3 \setminus \{0\}$

On étudie ensuite le morphisme

$$\begin{aligned} m_\beta : \mathbb{F}_8 &\longrightarrow \mathbb{F}_8 \\ x &\longmapsto \beta x. \end{aligned}$$

On écrit ensuite les images des points par m_β.

Point	Image
$1 = (1, 0, 0)$	$m_\beta(1, 0, 0) = (0, 1, 0) = 2$
$2 = (0, 1, 0)$	$m_\beta(0, 1, 0) = (0, 0, 1) = 4$
$3 = (1, 1, 0)$	$m_\beta(1, 1, 0) = (0, 1, 1) = 6$
$4 = (0, 0, 1)$	$m_\beta(0, 0, 1) = (1, 1, 0) = 3$
$5 = (1, 0, 1)$	$m_\beta(1, 0, 1) = (0, 0, 1) = 1$
$6 = (0, 1, 1)$	$m_\beta(0, 1, 1) = (1, 1, 1) = 7$
$7 = (1, 1, 1)$	$m_\beta(1, 1, 1) = (1, 0, 1) = 5$

TABLE 5 – Calcul des images de m_β

Remarque. On peut représenter la matrice de m_β dans la base $(1, \beta, \beta^2)$:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

il s'agit de la matrice compagnon du polynôme $X^3 + X + 1$, qui est le polynôme minimal de β (c'est à dire du morphisme m_β).

Donc le 7-cycle (1 2 4 3 6 7 5) est un automorphisme car par linéarité de m_β, la structure d'incidence est préservée. L'application m_β envoie une droite sur une droite, un plan sur un plan tout en préservant l'inclusion : c'est à dire l'incidence.

Exemple. Pour la suite on appellera p_i le vecteur de $\mathbb{F}_2^3$ correspondant au point i, où i parcourt les entiers de 1 à 7. Choisissons arbitrairement trois points non alignés p_1, p_2 et p_4. Justifions qu'il y a un automorphisme qui envoie 1 sur p_1, 2 sur p_2, 4 sur p_4. On complète notre plan avec le point $p_5 = p_1 + p_4$ pour former la droite $(1, 4, 5)$. Dans le même temps, on construit le point $p_3 = p_1 + p_2$ et on forme la droite $(1, 2, 3)$. Il nous reste maintenant à compléter les droites $(4, 7, 3)$ et $(5, 7, 2)$ ainsi que les droites $(5, 6, 3)$ et $(1, 7, 6)$. Pour trouver les images de 6 et 7, on réapplique notre calcul : $p_7 = p_5 + p_2 = p_4 + p_3$. Et donc sachant que $p_7 = p_1 + p_\beta$, on a $p_6 = p_1 + p_7$. On retrouve ainsi un automorphisme du plan de Fano (1) présenté plut tôt, il y en au moins 168.

L'argument de linéarité montre plus généralement que tout élément de $\mathrm{GL}_3(\mathbb{F}_2)$ induit un automorphisme de $\mathbb{P}^2(\mathbb{F}_2)$. On voit directement que ces derniers agissent sur $S(2, 3, 7)$ car ils envoient une droite sur une droite et un plan sur un plan. Ainsi, il y a conservation de la structure d'incidence.

Proposition. *Le groupe d'automorphisme du plan de Fano est* $\mathrm{GL}_3(\mathbb{F}_2)$ *et son ordre est* 168.

Démonstration. Montrons que la donnée de trois points non alignés (ce qu'on appelle un ovale) permet la reconstruction du plan de Fano. Il est important de considérer qu'un ovale est exactement une base de $\mathbb{P}^2(\mathbb{F}_2)$ car deux vecteurs sont linéairement indépendants s'ils sont différents et trois vecteurs sont linéairement indépendants s'ils ne sont pas tous les trois alignés ce qui revient à dire $u \neq v + w$ (cf. exemple plus tôt). Pour le premier point, nous n'avons aucune contraire sur le choix de ce dernier. Pour le deuxième point, une seule contrainte s'impose à nous : il nous est interdit de prendre le premier point. Enfin, il est interdit de choisir le troisième sur la droite contenant les deux premiers. Ce qui amène le nombre de choix de ces trois points à $7 \times 6 \times 4 = 168$. Ce nombre correspond aux nombre des bases de $\mathbb{F}_2^3$. Tout choix de trois points amène donc à un automorphisme car ils forment une base de $\mathbb{F}_2^3$. Quand nous fixons trois points, l'incidence est préservé, deux points permettent l'identification du troisième et nous pouvons vérifier que trois points sont alignés si leur somme est nulle.

Tout automorphisme σ est additif car si $u = v + w$, alors $u + v + w = 0$, c'est à dire u, v et w sont alignés. Il en va de même pour leur image par σ, si bien que $\sigma(u) = \sigma(v) + \sigma(w)$. Comme $\mathbb{F}_2$ est un corps premier, l'additivité implique la linéarité. D'où, le groupe des automorphismes du plan de Fano est $\mathrm{GL}_3(\mathbb{F}_2)$. □

2 Le groupe de Mathieu M_{12}

Si la lectrice souhaite reprendre certaines notions liés à la théorie des groupes, nous l'invitons à se référer à la partie consacrée dans l'annexe (A.1).

2.1 Système de Steiner $S(5, 6, 12)$: existence et unicité

On admet l'existence d'un système de Steiner $S(5, 6, 12)$ et qu'il est unique à isomorphisme/équivalence près.

Théorème. Il existe un système de Steiner $S(5, 6, 12)$ unique à isomorphisme près.

2.2 Définition du groupe de Mathieu M_{12}

Définition (groupe de Mathieu M_{12})**.** On définit le groupe de Mathieu M_{12} comme le groupes des automorphismes d'un et donc de n'importe quel système de Steiner $S(5, 6, 12)$ bien défini à isomorphisme près.

Remarque. Le groupe M_{12} est simple, sporadique et on verra qu'il est cinq fois transitif sur 12 points. Il est aussi le groupe des automorphismes pour une matrice de Hadamard de taille 12×12. Et le groupe des automorphismes du code de Golay ternaire est un groupe d'ordre $2|\mathrm{M}_{12}|$ qui admet M_{12} comme quotient.

Dans cette partie, nous allons montrer la proposition suivante

Proposition. *Le groupe* M_{12} *agit 5 fois transitivement sur douze points.*

Démonstration. La démonstration est faite à l'aide de notre programme informatique. Pour débuter, nous prenons deux quintuplets ordonnés $x = \{x_0, x_1, x_2, x_3, x_4\}$ et $y = \{y_0, y_1, y_2, y_3, y_4\}$, et nous réalisons une application σ telle que $\forall i, \sigma(x_i) = y_i$. Nous avons montré précédemment grâce au triangle d'intersection, mais nous le vérifions ici encore, que ces deux quintuplés sont contenus dans un seul et unique bloc qu'on nomme respectivement b_0 et B_0.

Pour calculer l'image des douze points par σ, nous allons prendre une paire disjointe π de b_0, cette paire est contenue dans trente blocs de $S(5, 6, 12)$. Ensuite, sur ces trente blocs, nous retirons π pour obtenir trente quadruplets, et il y a d'après le triangle d'intersection trois quadruplets q_1, q_2 et q_3 parmi ces trente qui sont contenus dans b_0. (calculs vérifiés par la fonction `quadruplet_paires` et la fonction `image_pi`). Une fois les q_i récupérés nous associons leur coordonnés à celle de x (exemple : si $b_0 = \{0, 1, 2, 3, 4, 5\}$ et $q_1 = \{0, 1, 3, 5\}$, nous avons $q_1 = \{x_0, x_1, x_4, x_5\}$).

Sachant que $\sigma(x_i) = y_i$ nous pouvons donc calculer Q_i les quadruplets tels que $\sigma(q_i) = Q_i$. Les trois Q_i sont contenus dans B_0 et pour chaque Q_i il y a trois paires disjointes (donc neuf paires au total) $\pi_{i,1}, \pi_{i,2}, \pi_{i,3}$ de B_0 telles que Q_i et $\pi_{i,j}$ forment un bloc. La paire $\pi_{i,k}$ commune aux trois Q_i est l'image de π.

Pour identifier l'image d'un élément nous allons calculer l'image de deux paires π_1, π_2 distinctes de b_0 et qui possèdent exactement un élément en commun u. Le calcul précédent renvoie deux paires dont l'élément commun est l'image de u. Comme nous connaissons l'image des six premiers x_i, nous appliquons l'algorithme décrit plutôt sur les paires du bloc disjoint de b_0 (fonction `image_elt`. Nous avons bien défini σ. Pour étudier les permutations engendrées, la fonction `phi` utilise des commandes de Sage pour renvoyer les transpositions et cycles associés à σ.

A présent, notre code fixe un quintuplet ordonné x, pour chaque y, on calcule l'application σ associée et nous constatons qu'il y en a 95040 et on vérifie qu'elles conservent le système de Steiner. □

3 Du plan projectif sur $\mathbb{F}_3$ au code de Golay

Référence : [1], [2], [3]. Pour mieux comprendre ou revoir certaines notions liées à la théorie des codes, nous invitons la lectrice à lire la partie de l'annexe (A.2).

3.1 Construction de codes (isomorphe au code) de Golay à partir de $\mathbb{P}^2(\mathbb{F}_3)$

A partir d'ici, nous allons travailler avec Sage afin de programmer les objets nécessaires pour illustrer les résultats de certaines démonstrations mais surtout construire le groupe M_{12}.

3.1.1 Construction

En introduction, on construit les éléments du plan projectif $\mathbb{F}_3$. Constatant que toute droite vectorielle possède un unique vecteur directeur dont le coefficient non nul le plus à gauche vaut 1, on choisit pour a,$b \in \mathbb{F}_3$ les éléments de type $[1 : a : b]$ où, $[x : y : z]$ désigne la droite engendrée par $(x,y,z) \in \mathbb{F}_3 \setminus \{(0, 0, 0)\}$, puis $[0 : 1 : a]$ puis le triplet $[0 : 0 : 1]$ pour désigner les 13 éléments de notre plan.

On construit $\mathscr{L}$ de la manière suivante : pour $k \in \mathbb{P}^2(\mathbb{F}_3)$ (l'ensemble des droites vectorielles du plan projectif), on note l_k la droite projective correspondant au plan orthogonal à k pour le produit scalaire standard sur $\mathbb{F}_3^3$, défini pour $v, w \in \mathbb{F}_3^3$ par $\langle v, w\rangle = \sum_{i=0}^{2} v_i w_i$.

Nous définissons ensuite treize vecteurs h_ℓ (pour ℓ une droite vectorielle de $\mathbb{P}^2(\mathbb{F}_3)$). Chaque h_ℓ comprend quatre coordonnées non nulles, qui correspondent aux coordonnées des points des droites l_k. Un exemple très concret : pour la droite $l_k = [9, 10, 11, 12]$, on a donc $h_\ell = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$.

Une fois les treize h_ℓ définis, on définit le code $\mathscr{C}$ comme l'espace vectoriel engendré par les h_ℓ, pour $\ell \in \mathscr{L}$. Puis $\mathscr{C}'$ le sous-code de $\mathscr{C}$ formé des vecteurs de $\mathscr{C}$ dont la somme des composantes est nulle. Enfin nous terminons cette partie de construction avec la définition des codes $\mathscr{C}_p$ et $\mathscr{G}_p$. Pour $p \in \mathscr{P}$, on définit un sous-code $\mathscr{C}_p$ de $\mathscr{C}$ par

$$\mathscr{C}_p := \{v \in \mathscr{C} : v_p = -\sum_{i \in \mathscr{P}} v_i\}$$

. On définit $\mathscr{G}_p$ en supprimant la coordonnée p. Plus précisément, $\mathscr{G}_p = \pi_p(\mathscr{C}_p)$ où $\pi_p : \mathbb{F}_3^{13} \longrightarrow \mathbb{F}_3^{12}$; $(v_i) \longmapsto (v_i)_{i \neq p}$. On verra que $\dim \mathscr{C} = 7$, $\dim \mathscr{C}' = 6 = \dim \mathscr{C}_p$ pour tout p. Ainsi chaque $\mathscr{G}_p$ est un code de dimension 6 dans $\mathbb{F}_3^{12}$ qui se trouve être isomorphe au code de Golay ternaire étendu.

3.1.2 Propriétés

Afin de vérifier notre construction, nous vérifions la proposition suivante.

Proposition. *Soit $c \in \mathscr{C}$. Alors :*

1. $\displaystyle\sum_{p \in \mathscr{P}} {c_p}^2 = \Big(\sum_{p \in \mathscr{P}} c_p \Big)^2$;
2. $\mathrm{wt}(c) \equiv 0$ *ou* $1 \pmod 3$;
3. $c \in \mathscr{C}'$ *si et seulement si* $\mathrm{wt}(c) \equiv 0 \pmod 3$;
4. *pour chaque* $l \in \mathscr{L}$,
$$\sum_{p \in \mathscr{P}} c_p = \sum_{p \in \ell} c_p ;$$
5. $\mathscr{C}' = \mathscr{C}^{\perp}$;
6. $\dim \mathscr{C} = 7$ *et* $\dim \mathscr{C}' = 6$;
7. $\mathrm{wt}_{\min}(\mathscr{C}) = 4$ *et* $\mathrm{wt}_{\min}(\mathscr{C}') = 6$.

Démonstration. On pourrait copier la démonstration proposée dans l'article [1] mais on se propose plutôt de vérifier à l'aide d'un code informatique tous ces points. La démonstration des points 1 et 4 est faite informatiquement grâce à la commande `all` qui vérifie une assertion pour toutes les données d'un ensemble. Concernant les autres points, nous proposons d'étudier ci-dessous différents résultats exploitables.

Poids du vecteur c	0	4	6	7	9	10	12	13
Poids du vecteur $c \mod 3$	0	1	0	1	0	1	0	1

(a) Nombre de vecteurs de $\mathscr{C}$ par poids

Poids du vecteur c	0	6	9	12
Poids du vecteur $c \mod 3$	0	0	0	0

(b) Nombre de vecteurs de $\mathscr{C}'$ par poids

TABLE 6 – Tableaux présentant les différents poids trouvés dans $\mathscr{C}$ et $\mathscr{C}'$

La table 6, montre que le poids d'un vecteur dans $\mathscr{C}$ est 0 ou 1 modulo 3, ce qui prouve le point 2. De plus, en retirant la valeur 0 des deux tableaux, on peut constater que le poids minimal dans $\mathscr{C}$ est 4, que dans $\mathscr{C}'$ ce dernier vaut 6 : le point 7 est lui aussi démontré. Pour le point 3, nous débutons par vérifier que le poids de tous les vecteurs de $\mathscr{C}'$ est congru à 0 modulo 3. Puis la réciproque, c'est à dire nous regardons si tous les vecteurs de poids congru à 0 modulo 3 appartiennent à $\mathscr{C}'$. Ce qui est le cas et donc confirme le point 3. Pour vérifier les égalités du point 6, on exécute seulement la commande `dimension()` qui permet d'afficher la dimension de $\mathscr{C}$ et $\mathscr{C}'$. Le point 6 est donc finalement lui aussi démontré. Pour montrer le point 5 on procède de manière usuelle à l'instar des espaces vectoriels, en calculant le produit scalaire des vecteurs de bases de $\mathscr{C}$ et de $\mathscr{C}'$. Le produit scalaire est non dégénéré et l'égalité des dimensions nous assure que $\mathscr{C}$ et $\mathscr{C}'$ sont orthogonaux. C'est à dire $\mathscr{C}' = \mathscr{C}^{\perp}$. □

Cette proposition étant vérifiée, nous allons maintenant montrer le lien existant entre $\mathscr{G}_p$, les matrices d'Hadamard un $S(5, 6, 12)$, et le code de Golay.

3.1.3 Codes de Golay

Définition (code de Golay ternaire parfait)**.** Le code de Golay ternaire parfait est un $[11, 6, 5]_3$-code, c'est-à-dire un code linéaire avec des blocs de longueur 11 sur un espace de dimension 6, de poids minimum 5, sur $\mathbb{F}_3$.
Une matrice génératrice est

$$\left[\begin{array}{ccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 & 1 & 2 & 2 \end{array}\right].$$

Définition (code de Golay ternaire étendu)**.** Le code de Golay ternaire étendu est un $[12, 6, 6]$ code linéaire, il est obtenu à partir du code de Golay ternaire parfait en ajoutant la clé de contrôle zero-sum.
Une matrice génératrice est

$$\left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{array}\right].$$

Proposition. *Pour tout $p \in \mathscr{P}$, $\mathscr{G}_p$ est isomorphe au code de Golay ternaire étendu $\mathscr{C}_{12}$.*

Démonstration. La démonstration de ce point est faite en deux temps. Par un calcul prévu à cet effet, (dans la partie $\mathscr{G}_p$ isomorphe), nous sommes partis de la matrice d'une base de $\mathscr{G}_1$ appelée MAT puis par des opérations élémentaires nous sommes revenus à une matrice génératrice du code de Golay ternaire étendu GOL. Plus précisément, on exhibe des matrices monomiales P et Q telles que $\mathrm{P} \cdot \mathrm{MAT} \cdot \mathrm{Q} = \mathrm{GOL}$. Pour renforcer notre argument, nous vérifions que chaque ligne de la matrice $\mathrm{MAT} \cdot \mathrm{Q}$ appartient au code de Golay.

Pour ne pas réaliser cette manipulation douze fois supplémentaires, nous montrons pour un p quelconque à partir de la construction du jeu signé (défini un peu plus loin) en récupérant la matrice du chemin $[1, p]$ qu'on envoie bien $\mathscr{G}_1$ sur $\mathscr{G}_p$. □

Remarque. Conway, Elkies, et Martin se ramènent dans leur article à une caractérisation bien connue du code de Golay par Vera Pless [6] mais elle est bien plus compliquée que ce calcul.

Pour la suite de ce texte, il est utile d'afficher le nombre de vecteurs de $\mathscr{G}_p$ selon leur poids.

Poids du vecteur	0	1	2	3	4	5	6	7	8	9	10	11	12
Nombre de vecteurs associés	1	0	0	0	0	0	264	0	0	440	0	0	24

TABLE 7 – Nombre de vecteurs selon son poids

3.1.4 Système de Steiner

En reprenant la construction de $\mathscr{G}_p$, montrons que cette dernière définit un $S(5, 6, 12)$. Nous choisissons de manière arbitraire d'étudier $\mathscr{G}_0$ mais les résultats suivants restent vrais pour les autres p.

L'objectif est clair, montrer que toute partie à cinq éléments, qu'on nommera « pentade » est contenue dans un unique élément de S qu'on dénommera « bloc » ou « hexade ».

Proposition. *L'ensemble des supports des vecteurs de poids 6 dans $\mathscr{G}_0$, qu'on note W_6, est un système de Steiner $S(5, 6, 12)$.*

Démonstration. Notre programme informatique permet cette vérification grâce à la fonction `bloc`. Cette dernière renvoie pour une pentade donnée les blocs dans lesquels elle est contenue. Or, le résultat obtenu est toujours un seul bloc. Et l'exécution de la fonction à l'ensemble des pentades de $\mathscr{G}_0$ garantit la propriété caractéristique d'un système de Steiner. □

3.1.5 Matrice d'Hadamard

Dans cette section, nous étudions $\mathscr{G}_0$ (ici $p = 0$). Nous regardons également la table 3.1.3. Quelques remarques intéressantes à propos de ces nombres. Il n'y a qu'un seul vecteur de poids zéro : il s'agit du vecteur nul. Il y a 24 vecteurs de poids maximal, formés de douze paires de vecteurs opposés. Nous décidons de porter une attention particulière sur les 12 vecteurs de poids 24 ayant la première égale à 1 et nous retranscrivons en changeant d'anneau la matrice constituée (en lignes) de ces derniers :

$$H_0 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Regardons maintenant la définition d'une matrice d'Hadamard.

Définition (matrice d'Hadamard)**.** Une matrice d'Hadamard est une matrice carrée entière dont les coefficients sont tous 1 ou -1 et dont les lignes (ou les colonnes) sont toutes orthogonales entre elles, pour le produit scalaire standard.

Proposition. *La matrice H_0 est une matrice d'Hadamard.*

Démonstration. Nous vérifions aisément que les lignes sont toutes orthogonales deux à deux. De plus, les coefficients de la matrice sont bien des -1 ou 1. Cet argument peut être remplacé par ${}^tH_0H_0 = 12\mathrm{Id}$. Donc H_0 est une matrice d'Hadamard. □

4 Un jeu de taquin pour le groupe de Mathieu

Référence : [1].

4.1 Jeu de base

4.1.1 Description

Dans cette partie nous débutons par décrire le jeu sur le plan projectif $\mathbb{P}^2(\mathbb{F}_3)$. On numérote les droites et les points de $\mathbb{P}^2(\mathbb{F}_3)$ comme dans la table suivante,

$\overline{0} = \{9, 10, 11, 12\}$	$\overline{1} = \{2, 5, 8, 9\}$	$\overline{2} = \{1, 4, 7, 9\}$	$\overline{3} = \{6, 7, 8, 12\}$
$\overline{4} = \{2, 4, 6, 11\}$	$\overline{5} = \{1, 5, 6, 10\}$	$\overline{6} = \{3, 4, 5, 12\}$	$\overline{7} = \{2, 3, 7, 10\}$
$\overline{8} = \{1, 3, 8, 11\}$	$\overline{9} = \{0, 1, 2, 12\}$	$\overline{10} = \{0, 5, 7, 11\}$	$\overline{11} = \{0, 4, 8, 10\}$
$\overline{12} = \{0, 3, 6, 9\}$			

TABLE 8 – Droites de $\mathbb{P}^2(\mathbb{F}_3)$

On place douze pièces numérotées 1 à 12 sur les points de $\mathbb{P}^2(\mathbb{F}_3)$; cette configuration laisse un « trou » sur le treizième point, que l'on code par un 0. Pour toute cette partie, on note $\mathfrak{S}_{\mathscr{P}}$ le groupe des permutations de $\{0,\dots,12\} = \mathscr{P}$. Une position de jeu est codée par une permutation σ de $\mathfrak{S}_{\mathscr{P}}$, on a la pièce $\sigma(p)$ sur le point p. Un mouvement de jeu est une succession de mouvements « élémentaires ». On suppose le trou 0 au point p, on définit un mouvement « élémentaire » en choisissant $q \neq p$ tel que $l = \{p, q, r, s\}$ est la droite contenant p et q. Ce chemin noté $[p, q]$ correspond au déplacement de la tuile q sur le trou p ; le jeu échange de plus les tuiles r et s, où r et s sont les deux autres points de la droite l.

Avec l'écriture considérée, le mouvement $[p, q]$ correspond à une permutation $(p\ q)\ (r\ s) \in \mathfrak{S}_{13}$. Si la position du trou le permet, on peut ensuite définir l'enchaînement de mouvements par une suite de mouvements élémentaires qu'on notera

$$[p_0, p_1, \dots, p_n] = [p_{n-1}, p_n] \circ \cdots \circ [p_1, p_0].$$

Cette même suite définit la permutation

$$(p_{n-1}\ p_n)\ (r_n\ s_n) \cdots (p_0\ p_1)\ (r_1\ s_1)$$

où les points r_i et s_i sont les deux derniers points de la droite $\overline{p_{i-1}p_i}$. Par convention, le chemin $[p, p]$ est trivial et donc il y a douze mouvements légaux non triviaux pour chaque position du jeu.

Exemple. Le chemin/mouvement $[4, 6, 12, 1, 8, 4]$ est associé à la permutation

$$(4\ 8)\ (0\ 10) \circ (1\ 8)\ (3\ 11) \circ (12\ 1)\ (0\ 2) \circ (6\ 12)\ (7\ 8) \circ (4\ 6)\ (2\ 11) = (0\ 2\ 3\ 11\ 10)\ (1\ 12\ 6\ 8\ 7).$$

On dit ensuite que deux chemins sont *équivalents* s'ils induisent la même permutation. Il suit que tout chemin est équivalent à un chemin de longueur égale ou plus petite dans lequel trois points consécutifs ne sont pas alignés. On peut vérifier rapidement que si $l = \{p, q, r, s\}$, on a

$$[p, q, r] = (q\ r)\ (p\ s) \circ (p\ q)\ (r\ s) = (s, q)\ (p, r) = [s, q] = [p, r].$$

Un tel chemin sera dit *non dégénéré*. On parlera aussi de chemin *clos* ou *fermé* si ce chemin débute et se termine par le même point (c'est le cas du chemin proposé dans l'exemple).

Définition (groupoïde)**.** Soit X un ensemble. On appelle *groupoïde* sur X la donnée d'un ensemble $\mathbb{G}$ muni de deux applications $s, b : \mathbb{G} \longrightarrow X$ et d'une opération partiellement définie

$$\{(\gamma, \delta) \in \mathbb{G} \times \mathbb{G} : s(\gamma) = b(\delta)\} \longrightarrow \mathbb{G}$$

telle que pour $\gamma, \delta, \varepsilon \in \mathbb{G}$,

1. si $s(\gamma) = b(\delta)$ alors $b(\gamma \circ \delta) = b(\gamma)$ et $s(\gamma \circ \delta) = s(\delta)$;
2. si $(\gamma \circ \delta) \circ \varepsilon$ et $\gamma \circ (\delta \circ \varepsilon)$ ont un sens, ils sont égaux ;
3. $\forall p \in X, \exists \varepsilon_p$ tel que $\gamma \circ \varepsilon_p = \gamma$ et $\varepsilon_p \circ \delta = \delta$ quand les membres de gauche ont un sens ;
4. $\forall \gamma, \exists \gamma'$ tel que $\gamma \circ \gamma' = \varepsilon_{b(\gamma)}, \gamma' \circ \gamma = \varepsilon_{s(\delta)}$.

On définit le groupoïde $\mathbb{M}_{13}$ comme l'ensemble des chemins $[p_n, \cdots, p_0]$ avec $s(\gamma) = p_0$, $b(\gamma) = p_n$ et $\circ$ l'opération de concaténation. La permutation associée à γ, disons $\sigma(\gamma)$ permet de définir

$$\mathrm{M}_{13} = \{\sigma(\gamma) : \gamma \in \mathbb{M}_{13}\}.$$

Lorsqu'une permutation de $\mathfrak{S}_{13}$ fixe 0, on l'identifie à une permutation de $\mathfrak{S}_{12} = \mathfrak{S}_{\mathscr{P}\setminus\{0\}}$. Ces permutations forment un sous-groupe de $\mathfrak{S}_{12}$ nommé « groupe du jeu de base » et noté G_{bas}. On appellera M_{13} l'ensemble de toutes les séquences de mouvements avec $p_0 = 0$. À noter que $G_{bas} \subsetneq \mathrm{M}_{13}$. Cependant M_{13} n'est pas un groupe car les mouvements possibles pour une position donnée dépendent de la localisation du trou, et donc on ne peut pas toujours réaliser un enchaînement de séquences : M_{13} est une réunion de classes modulo G_{bas}.

4.1.2 Propriétés

On établit un premier lien entre le jeu de taquin et le groupe de Mathieu.

Proposition. *Le groupe G_{bas} contient un sous-groupe isomorphe au groupe de Mathieu* M_{12}.

Démonstration. La démonstration résulte de notre programme : nous avons choisi plusieurs chemins fermés partant de 4, puis nous avons calculé les permutations associées dans G_{bas} afin d'exhiber le groupe engendré. On vérifie alors doublement que le groupe obtenu est isomorphe à M_{12} :

— dans un premier temps, on fait calculer l'ordre du groupe engendré (on trouve 95 040) et on montre que les permutations préservent le système de Steiner W_6 des supports des vecteurs de poids 6 de $\mathscr{G}_0$; ce dernier fait sera expliqué par la variante signée du jeu présentée dans la partie suivante ;

— dans un second temps, on fait vérifier directement à Sage que le groupe est isomorphe au groupe de Mathieu M_{12} grâce à la commande `is_isomorphic`. □

On montrera plus tard que G_{bas} est en fait isomorphe au groupe de Mathieu M_{12}.

4.2 Jeu signé

Dans cette partie on joue à une variante du jeu de base. Au lieu d'associer une permutation à un chemin, on associe une matrice monomiale qui se trouve *in fine* préserver les $\mathscr{G}_p$.

4.2.1 Description

Dans ce jeu, chaque tuile possèdera deux faces. Supposons que le trou est au point p. Nous choisissons $q \neq p$ tel que $l = \{p, q, r, s\}$ est la droite de $\mathbb{F}_3^3$ (contenant p et q). Le mouvement $[p, q]$ déplace la tuile q sur le trou p, échange les tuiles r et s et les retourne. La notion de séquences de mouvements élémentaires existe aussi dans ce jeu et induit une permutation « signée » ou une matrice monomiale sur l'ensemble $\mathscr{P}$.

Exemple. Dans le jeu signé, le chemin/mouvement $[4, 6, 12, 1, 8, 4]$ est associé à la matrice monomiale

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Le groupe des permutations signés de $\mathscr{P}\backslash\{0\}$ par les séquences de mouvements fermés sera nommé le groupe du jeu signé G_{sgn}. L'ensemble des permutations signées définies par des chemins qui commencent par $p_0 = 0$ est appelé $2\mathrm{M}_{13}$.

On construit ainsi le groupe des automorphismes du code de Golay, un groupe qui admet M_{12} comme quotient par un sous-groupe d'ordre 2.

4.2.2 Propriétés

Le jeu étant présenté, nous pouvons nous intéresser aux propositions suivantes.

Lemme. *Le groupe G_{sgn} préserve le code $\mathscr{G}_0$.*

Démonstration. Par construction, les éléments du jeu signé sont des matrices monomiales. On commence par vérifier que pour $p, q \in \mathscr{P}$, la matrice associée au mouvement élémentaire $[p, q]$ envoie $\mathscr{G}_p$ sur $\mathscr{G}_q$, ce que l'on fait par calcul (cf. partie $\mathscr{G}_p$ isomorphe le retour). Pour montrer le lemme, il suffit de se rappeler que G_{sgn} est engendré par les matrices monomiales associées à un chemin fermé issu de 4, qui par composition envoie donc $\mathscr{G}_0$ sur $\mathscr{G}_0$. □

D'après le lemme, le groupe G_{sgn} agit par automorphismes de $\mathscr{G}_0$. Or, si $A \in \mathrm{Aut}(\mathscr{G}_0)$ et $v \in \mathscr{G}_0$, alors $\mathrm{wt}(Av) = \mathrm{wt}(v)$. En particulier, si $\mathrm{supp}(v) \in \mathrm{W}_6$, alors $\mathrm{supp}(Av) \in \mathrm{W}_6$ également. On peut donc définir une action de $\mathrm{Aut}(\mathscr{G}_0)$ sur le $S(5, 6, 12)$ qu'est W_6 : pour $A \in \mathrm{Aut}(\mathscr{G}_0)$ et un bloc $b \in \mathrm{W}_6$, on choisit $v \in \mathscr{G}_0$ tel que $b = \mathrm{supp}(v)$ et on pose $A \cdot b = \mathrm{supp}(Av)$. On obtient un morphisme $\varphi : \mathrm{Aut}(\mathscr{G}_0) \to \mathrm{Aut}(W_6)$.

En d'autres termes, le morphisme φ revient à oublier les signes dans la matrice monomiale, ce qui donne une matrice de permutation, à qui on associe la permutation.

En particulier, par construction, le groupe du jeu basique, G_{bas}, est l'image par φ du groupe du jeu signé, G_{sgn}. Cela entraîne que G_{bas} est inclus dans le groupe $\mathrm{Aut}(W_6)$, qui est isomorphe au groupe de Mathieu M_{12}. Vu la proposition 4.1.2, cela signifie que G_{bas} est *égal* à $\mathrm{Aut}(\mathrm{W}_6)$.

Proposition. *Le groupe G_{sgn} est isomorphe au groupe des automorphismes du code de Golay. Le quotient de G_{sgn} par $\{\pm \mathrm{I}_{12}\}$, qui est isomorphe à G_{bas}, est isomorphe au groupe de Mathieu* M_{12}.

Démonstration. On commence par montrer par un calcul que le noyau de φ est d'ordre 2 : pour cela, on regarde quelles matrices diagonales stabilisent $\mathscr{G}_0$: il se trouve qu'il n'y a que $\pm \mathrm{I}_{12}$. Il en résulte que $|\mathrm{Aut}\,\mathscr{G}_0| = 2\,|\mathrm{M}_{12}|$.

Or on peut trouver un chemin explicite dont la matrice monomiale associée est $-\mathrm{I}_{12}$; autrement dit, G_{sgn} contient le noyau de φ. On peut aussi trouver deux chemins dont les matrices monomiales associées engendrent un sous-groupe de G_{sgn} d'ordre $2\,|\mathrm{M}_{12}|$. Il en résulte que $G_{sgn} = \mathrm{Aut}\,\mathscr{G}_0$ et que

$$G_{bas} \simeq G_{sgn}/\{\pm \mathrm{I}_{12}\} \simeq \mathrm{Aut}(\mathrm{W}_6) \simeq \mathrm{M}_{12}.$$

□

4.3 Jeu dual

Faute de temps, cette partie est très sommaire et n'a pas été implémentée. Dans le jeu dual, on place des tuiles sur tous les points de $\mathbb{P}^2(\mathbb{F}_3)$ sauf un et sur toutes les droites sauf une et on les permute simultanément par une succession de mouvements élémentaires. La seule contrainte est que le point où est le trou des points appartienne à la droite où est le trou des droites. Sous cette contrainte, un chemin fermé permet de définir deux permutations, l'une des points, l'autre des droites. L'intérêt de cette construction est double :

— si les numérotations des droites et des points sont compatibles (au sens où le point j appartient à la droite l_k si et seulement si le point k appartient à la droite l_j), échanger les deux permutations donne lieu un automorphisme extérieur de M_{12}, qui reçoit ainsi une construction naturelle (indépendante de choix, si ce n'est celui de numérotations de $\mathbb{P}^2(\mathbb{F}_3)$) ;

— on peut d'autre part montrer que l'action de la permutation des points (resp. des droites) sur les lignes (resp. les colonnes) de la matrice d'Hadamard construite la préserve : on obtient ainsi une autre réalisation classique du groupe M_{12} comme groupe d'automorphismes d'une matrice d'Hadamard 12×12.

A Annexes

A.1 Vocabulaire des actions de groupes

Débutons par quelques rappels sur les groupes.

Définition (groupe)**.** On appelle *groupe* un couple $(G, \cdot)$ formé d'un ensemble G muni d'une loi de composition interne, appelée produit, vérifiant :

1. l'associativité $\forall x, y, z \in G$, $x(yz) = (xy)z$;
2. l'existence d'un élément neutre e tel que, $\forall x \in G$, $ex = xe = x$;
3. l'existence d'un élément symétrique tel que, $\forall x \in G, \exists x^{-1} \in G$, $xx^{-1} = x^{-1}x = e$.

Définition (sous-groupe)**.** On appelle un *sous-groupe* de $(G, \cdot)$ une partie non vide H de G, stable par produit et passage à l'inverse.

Exemple. L'ensemble $\mathbb{N}$ muni de la loi additive $+$ n'est pas un groupe car à part 0, aucun autre élément n'admet un élément opposé. Au contraire, $(\mathbb{Z}, +)$ est bien un groupe.

On va maintenant définir les actions de groupe.

Définition (action de groupe)**.** Soit $(G, \cdot)$ un groupe d'élément neutre e et soit E un ensemble.
On appelle *action* (ou *opération*) du groupe G sur E une application :

$$\begin{aligned} G \times E &\longrightarrow E \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

qui vérifie les deux propriétés suivantes :

1. $\forall x \in E$, $e \cdot x = x$;
2. $\forall (g, g') \in G^2$, $\forall x \in E$, $g' \cdot (g \cdot x) = (g'g) \cdot x$

Voici trois exemples d'actions de G sur G

1. conjugaison : $g \cdot x = gxg^{-1}$ pour tout $(g, x) \in G \times G$;
2. translation à gauche $g \cdot x = gx$;
3. translation à droite $g \cdot x = xg^{-1}$.

Définition (sous-groupe normal)**.** On dit qu'un sous-groupe H d'un groupe G est *normal* ou *distingué* dans G s'il est stable par conjugaison, c'est-à-dire si : $\forall h \in H$, $\forall x \in G$, $xhx^{-1} \in H$.

On note alors $H \trianglelefteq G$.

Exemple. Pour un groupe $(G, \cdot)$, où e désigne l'élément neutre de $\cdot$ dans G. Les sous-groupes G et $\{e\}$ sont toujours des sous groupes normaux.

Définition (groupe simple)**.** On dit qu'un groupe (non trivial) est *simple* lorsqu'il ne possède que deux sous groupes normaux : lui-même et le sous-groupe trivial.

Exemple. Le groupe spécial des matrices orthogonales $SO_3(\mathbb{R})$ et le groupe alterné $\mathscr{A}_5$ sont deux groupes simples.

Enfin, nous proposons d'introduire cinq dernières propriétés pour analyser les actions de groupes.

Définition (types d'action)**.** Une action est dite :

1. *fidèle*, si pour $g \in G$, tel que pour tout $x \in E$, $g \cdot x = x$, on a $g = e$;
2. *libre*, si pour $g \in G$ et $x \in E$ avec $g \neq e$, on a $g \cdot x \neq x$;
3. *transitive*, si pour tout $x, y \in E$, on a l'existence d'un $g \in G$ tel que $g \cdot x = y$;
4. *simplement transitive*, si elle est fidèle et libre.
5. *r fois transitive* si sur un ensemble E (d'au moins r éléments) l'action correspondante sur l'ensemble des r-uplets d'éléments distincts est transitive. Cela signifie que pour r points distincts $x_1, \ldots, x_r$ et r points distincts $y_1, \ldots, y_r$ dans E, il existe toujours au moins un élément g du groupe tel que pour tout $i \in \{1, \ldots, r\}$ on ait $g \cdot x_i = y_i$.

Exemple. L'action de $\mathrm{GL}_3(\mathbb{F}_2)$ sur $\mathbb{F}_2^3 \setminus \{(0,0,0)\}$ est 2 fois transitive. (voir (1.2)).

A.2 Vocabulaire des codes

Définition (code linéaire)**.** On appelle *code linéaire* de longueur n et de dimension k sur $\mathbb{F}_q$, un sous-espace vectoriel C de dimension k de $\mathbb{F}_q^n$.

Définition (code détecteur/correcteur)**.** Un code $(n,\ k)$ est dit *t-détecteur* (resp. *t-correcteur*) s'il permet de détecter (resp. corriger) toute erreur portant sur t chiffres ou moins lors de la transmission d'un mot de code de n chiffres.

Exemple. Pour un code de 7 bits, on peut en ajouter un huitième pour contrôler la parité des sept qui le précède. Il s'agit alors d'un code $(8, 7)$ qui est 1-détecteur (car il détecte une erreur sur au moins un bit) et 0-correcteur (car il ne permet pas d'identifier au moins un bit erroné pour le corriger).

Définition (automorphisme d'un code)**.** On appelle *automorphisme d'un code* $C \subset \mathbb{F}_q^n$, l'ensemble des matrices monomiales A de taille $n \times n$ telles que $AC \subset C$.

Ces notions peuvent être associées au support puis le poids d'un vecteur.

Définition (support)**.** On appelle *support* du vecteur v l'ensemble des composantes non nulles de v. Autrement dit, $\text{supp}(v) = \{i \in \{1, \ldots, n\} | v_i \neq 0\}$.

Définition (poids de Hamming)**.** On appelle *poids* d'un vecteur v le nombre de composantes de v différentes de 0. On le note $\text{wt}(v)$ et on voit directement que $\text{wt}(v) = |\text{supp}(v)|$.

Le poids minimal d'un code, qu'on notera $\text{wt}_{\min}(\mathscr{C})$, est la valeur minimale du poids d'un vecteur non nul, $\text{wt}_{\min}(\mathscr{C}) = \min\{\text{wt}(v) : v \in \mathbb{C}\}$.

Définition (distance de Hamming)**.** On définit la distance de Hamming, notée $d_H(x, y)$, le nombre de composantes pour lesquelles x et y diffèrent, i.e

$$d_H(x, y) = \big|\{i \in \{1, \ldots, n\} : x_i \neq y_i\}\big|.$$

Exemple. Soit $F = \{v \in \mathbb{F}_2^8 : \sum_{i=0}^{7} v_i = 0\}$ un code. Il est 1-détecteur et on peut le voir rapidement car si on obtient $\forall v \in F, \forall w \in \mathbb{F}_2^8, d_H(v, w) = 1$ cela signifie que $w \notin F$. Cependant, impossible de localiser la ou les composantes de w qui empêchent son appartenance à F. Il est donc 0-correcteur.

Définition (matrice génératrice d'un code)**.** Soit C un code (n, k) sur $\mathbb{F}$. On appelle *matrice génératrice d'un code* C, la matrice d'une application linéaire $\phi : \mathbb{F}^k \longrightarrow \mathbb{F}^n$ telle que$\phi(\mathbb{F}^k) = C$.

Définition (clé de contrôle)**.** On appelle *clé de contrôle* une suite de symboles associés à un code permettant d'assurer sa validité, i.e le fait qu'il ne contient pas d'erreurs.

Définition (matrice monomiale)**.** On appelle matrice *monomiale*, une matrice carrée pour laquelle chaque ligne et colonne admet exactement un élément non nul.

Remarque. Les matrices monomiales sont très utiles dans notre texte car elles sont exactement les bijections linéaires qui préservent la distance de Hamming. Il est clair que la permutation de coordonnées différentes de 0 ne va pas changer le nombre de zéros présent dans le vecteur étudié.

Références

[1] John H. Conway, Noam D. Elkies et Jeremy L. Martin : The Mathieu group M_{12} and its pseudogroup extension M_{13}. *Experiment. Math.*, 15(2):223–236, 2006.

[2] Michel Demazure : *Cours d'algèbre*, volume 1 de *Nouvelle Bibliothèque Mathématique*. Cassini, Paris, 1997. Primalité. Divisibilité. Codes.

[3] Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier et Sébastien Varrette : Théorie des codes. *Dunod, Paris*, 2007.

[4] Marshall Hall : *Combinatorial Theory*. Wiley Classics Library. Wiley, 2011.

[5] Graham Higman Peter J. Cameron : From M_{12} to M_{24}. 2015.

[6] Vera Pless : On the uniqueness of the Golay codes. *Journal of Combinatorial Theory*, 5(3):215–228, 1968.