LES JEUX DE TAQUIN ET M_{12}

Elias Giraud-Audine, Quentin Palazon

Résumé. — Le but premier de notre mémoire est d'étudier la construction du groupe sporadique M_{12} donnée par Conway [**1**], qui est inspirée du jeu de taquin de Sam Loyd.

Cela nous a amené à nous poser une question connexe. Dans une première partie nous généraliserons le taquin à des graphes finis et nous caractériserons la structure des groupes de permutations qu'ils engendrent. Nous montrerons que ces groupes sont exactement les produits de $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

La deuxième partie constitue le cœur de notre mémoire sur le taquin de Conway. Nous y verrons que M_{12} agit sur 12 des 13 points de $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$. Cette aventure nous fera découvrir les codes de Golay et les systèmes de Steiner.

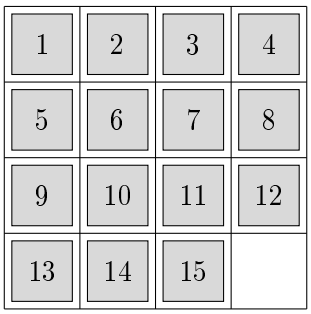
Enfin, nous justifierons la construction traditionnelle de M_{12} en montrant notamment l'unicité du système de Steiner $S(5,6,12)$. Nous expliciterons pour cela un automorphisme extérieur de $\mathfrak{S}_6$ en nous appuyant sur [**2**].

Les trois parties de ce mémoire sont relativement indépendantes et la dernière, plus technique, peut être considérée une annexe.

Table des matières

PARTIE I. LES GROUPES DE TAQUIN

1. Introduction



Le jeu du taquin de Sam Loyd est constitué de 15 jetons numérotés placés sur un plateau de 4×4 cases, avec une case vide appelée case blanche. Le but est d'ordonner les jetons en les faisant coulisser. Les *suites de coups closes* (qui ramènent la case blanche en position initiale) engendrent alors un sous-groupe de $\mathfrak{S}_{15}$. Il est connu que ce groupe est $\mathfrak{A}_{15}$, nous retrouverons ce résultat.

Une généralisation naturelle de ce jeu consiste à remplacer le plateau par un graphe non orienté où l'on peut déplacer les jetons le long des arêtes.

On commence par définir $T(G, s_0)$ le *groupe de taquin* du graphe G pointé en s_0. Ce dernier ne dépend pas de s_0 à isomorphisme près si le graphe est connexe. On s'intéresse ensuite à quelques graphes particuliers, dont le graphe G_{ex} en figure 1 qui nous donne une belle réalisation d'un morphisme injectif non trivial de $\mathfrak{S}_5$ dans $\mathfrak{S}_6$.

Dans la dernière section, nous démontrons que les groupes de taquin sont exactement les produits directs finis de $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$ et $\mathfrak{A}_n$ à isomorphisme près.

Il se trouve que ces groupes avaient en fait déjà été étudiés [**3**].

2. Groupes de taquin

Dans toute la suite on s'intéressera à un graphe $G = (S, A)$ fini non orienté connexe (où S sont les sommets et $A \subseteq \mathcal{P}_2(S)$ les arêtes), on fixe également un sommet $s_0 \in S$.

Initialement, on place sur les sommets (ou cases) de G des jetons étiquetés par les éléments de S correspondants, sauf sur le sommet s_0. La case sans jeton est appelée la *case blanche* (en s_0 initialement). Soit u la case blanche, v un sommet adjacent. On peut alors effectuer le coup $[u, v]$ qui consisté à déplacer le jeton de la case u sur la case v.

Un coup $[u, v]$ induit la permutation $\langle u, v\rangle = (u\ v) \in \mathfrak{S}_S$, et une suite de coups $[u_0, u_1]$, $[u_1, u_2]$, … $[u_{n-1}, u_n]$ qu'on notera $[u_0, u_1, \dots, u_n]$ correspond donc à la permutation $\langle u_0, u_1, \dots, u_n\rangle = (u_n\ u_{n-1}) \circ \cdots \circ (u_2\ u_1) \circ (u_1\ u_0)$.

Une suite de coups débutant et terminant en s_0 est dite *close*.

On note $T(G, s_0) \subseteq \mathfrak{S}_S$ l'ensemble des permutations correspondant aux suites de coups closes. Il forme manifestement un sous-groupe de $\mathfrak{S}_S$ stabilisant s_0, il sera naturel de le voir dans $\mathfrak{S}_{S\setminus\{s_0\}}$.

Remarque 2.1. — La parité de la longueur d'une suite de coups (nombre de coups) correspond à la signature de la permutation de $\mathfrak{S}_S$ associée à cette suite.

Proposition 2.2. — *Les groupes $T(G, u)$ pour $u \in S$ sont conjugués dans $\mathfrak{S}_S$ et en particulier isomorphes.*

Démonstration. — Soient $u, v \in S$, par connexité il existe un chemin $(u = u_0, u_1, \ldots, u_k = v)$. On a alors, en observant que $\langle u_0, u_1, \ldots, u_n\rangle$ est inverse à $\langle u_n, u_{n-1}, \ldots, u_0\rangle$:

$$T(G, u) = \langle u_n, u_{n-1}, \ldots, u_0\rangle \circ T(G, V) \circ \langle u_n, u_{n-1}, \ldots, u_0\rangle^{-1}$$

□

3. Cas de base

3.1. Cycles

Proposition 3.1. — *Si G est un cycle de taille $n \geqslant 3$, alors*

$$T(G, s_0) \simeq \mathbb{Z}/(n-1)\mathbb{Z}$$

Démonstration. — Soit $s_0, s_1, \ldots, s_{n-1}$ le cycle. On constate que la suite close $[s_0, s_1, \ldots, s_{n-1}]$ définit le $(n-1)$-cycle $(s_1\ s_2 \ldots s_{n-1})$ qui engendre $T(G, s_0)$. □

3.2. Graphe exceptionnel

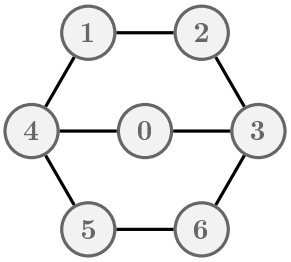


FIGURE 1. Le graphe exceptionnel G_{ex}

Traitons le cas du graphe G_{ex} (figure 1).

Proposition 3.2. — *Le groupe $T(G_{ex}, 0)$ est isomorphe à $\mathfrak{S}_5$ et agit transitivement sur $S \setminus \{0\}$.*

Ce graphe réalise donc une injection non triviale de $\mathfrak{S}_5$ dans $\mathfrak{S}_6$!

Démonstration. — Le groupe $T(G_{ex}, 0)$ est manifestement engendré par les cycles $\mu = (1\ 2\ 3\ 4)$ et $\nu = (3\ 4\ 5\ 6)$ (d'où la transitivité).

Soit $X = S \setminus \{0\}$, on appelle *synthème* une partition de X en 3 paires. On considère les 5 synthèmes a, b, c, d, e en figure 2, qui forment une partition $R = \{a, b, c, d, e\}$ des paires de X. On remarque alors que R est stable par l'action naturelle de $T(G_{ex}, 0)$ sur les synthèmes, en effet μ agit comme $(a\ b\ c\ d)$ (flèches bleues) et ν comme $(e\ d\ c\ b)$ (flèches vertes). On en déduit $\Phi : T(G_{ex}, 0) \longrightarrow \mathfrak{S}_R$.

- Montrons que cette action est fidèle (Φ injective). Soit $\sigma \in T(G_{ex}, 0)$ agissant trivialement sur R.

  Remarquons d'abord que σ est involutive. En effet soit $i \in X$, si $i \neq \sigma(i)$, il existe une synthème A de R contenant $\{i, \sigma(i)\}$. Comme A est stabilisée, les paires $\{i, \sigma(i)\}$ et $\{\sigma(i), \sigma^2(i)\}$ sont dans A donc coïncident et $\sigma^2(i) = i$.

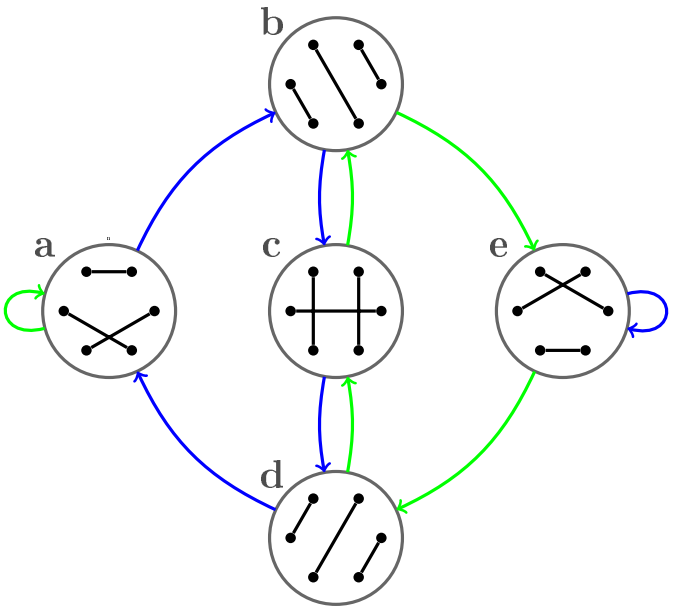


FIGURE 2. Synthèmes

De plus, chaque synthème de R possède une paire stabilisée par σ. En effet, si σ envoie une paire $\{i,j\}$ sur une paire différente $\{\sigma(i),\sigma(j)\}$, comme σ est involutive, ces deux paires sont échangées et la troisième est fixée.

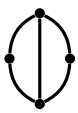
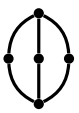
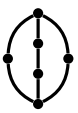
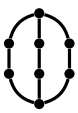
On se donne donc une paire fixée par synthème. Il existe deux paires d'intersection non vide $\{i\}$, qui est donc fixé par σ. Pour $j \neq i$, il suffit de considérer la synthème contenant $\{i,j\}$ pour voir que j est également fixé. On a montré que $\sigma = \mathrm{Id}_X$.

- Montrons que Φ est surjective. On a en effet :
  — $\Phi(\mu) = (a\ b\ c\ d)$ est d'ordre 4
  — $\Phi(\nu^{-1}\mu) = (a\ e\ d)$ est d'ordre 3
  — $\Phi(\nu\mu) = (a\ c\ e\ b\ d)$ est d'ordre 5
  Donc $\Phi(G_{ex})$ est d'ordre au moins 60 (d'indice 2) et n'est pas inclus dans $\mathfrak{A}_R$ car $\Phi(\mu)$ est impaire.

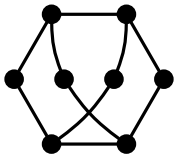
□

3.3. Graphes particuliers

Les graphes suivants sont utiles pour la suite, leurs groupes de taquins peuvent être démontrés à la main ou informatiquement. On remarquera que G_{ex} en fait partie.

						
$\mathfrak{S}_3$	$\mathfrak{S}_4$	$\mathfrak{A}_5$	$\mathfrak{A}_4$	$\mathfrak{S}_5$	$\mathfrak{S}_5$ (!)	$\mathfrak{A}_7$

On considère aussi $\widehat{G}_{ex}$ le graphe suivant de groupe taquin $\mathfrak{S}_7$:



3.4. Graphes lunettes

***Définition 3.3* (Adjonction de chemin).** — Soit $(s_0, s_1, \dots, s_n)$ un chemin et $G = (S, A)$ un graphe tels que :
- $n > 1$ ou l'arête $\{s_0, s_n\}$ n'est pas dans G
- Les sommets $s_0, \dots, s_n$ sont distincts
- $s_0, s_n \in G$ et ce sont les seuls du chemin

On appelle adjonction de $(s_0, s_1, \dots, s_n)$ à G le graphe

$$(S \sqcup \{s_2, \dots, s_{n-1}\}, A \sqcup \{\{s_i, s_{i+1}\} \mid 0 \leqslant i < n\})$$

Définition 3.4. — On appelle *graphe lunette* l'adjonction d'un chemin à un cycle.

Remarque 3.5. —
- Un tel graphe possède exactement deux sommets de degré 3 et est de taille au moins 4.
- On peut toujours supposer que le chemin adjoint n'est pas réduit à une arrête quitte à changer le cycle.

Exemple 3.6. — Le graphe G_{ex} est un graphe lunette.

Lemme 3.7. — *Soit G un graphe lunette obtenu par adjonction d'un chemin $(s_0, s_1, \dots, s_n)$. Alors $T(G, s_0)$ agit n-transitivement sur $S \setminus \{s_0\}$.*

Démonstration. — On montre par récurrence sur k que $T(G, s_0)$ agit k-transitivement pour tout $0 \leqslant k \leqslant n$.
- Initialisation : Rien à faire.
- Hérédité : On adopte les notations de la figure 3, où μ et ν sont deux cycles qui engendrent $T(G, s_0)$.

  Soient $a_1, a_2, \dots, a_k \in S \setminus \{s_0\}$. Par hypothèse de récurrence il existe $\sigma \in T(G, s_0)$ tel que $\forall i < k$, $\sigma(a_i) = s_i$.

  Si a_k est déjà envoyé par σ dans le cycle μ, en appliquant μ suffisamment de fois on l'envoie en t.

  Ensuite en appliquant $n - k + 1$ fois ν, on fait passer $a_1, \dots, a_{k-1}$ de $s_1, \dots, s_{k-1}$ à $s_{n-k+1}, \dots, s_{n-1}$. Si a_k passe en s_n durant cette opération, on applique μ pour le faire passer en t.

  Finalement, il reste à appliquer $\nu^{-(n-k+1)}\mu^{-1}$ pour envoyer $a_1, \dots, a_{k-1}, a_k$ en $s_1, \dots, s_{k-1}, s_k$.

□

Lemme 3.8. — *Soit G un graphe lunette non isomorphe à G_{ex}, alors*

$$T(G, s_0) \supseteq \mathfrak{A}_{S \setminus \{s_0\}}$$

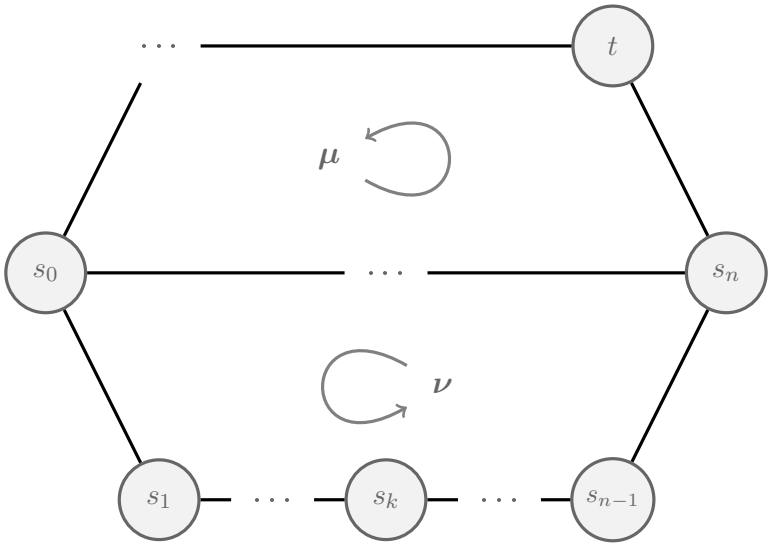


FIGURE 3. Notations du graphe lunette

Démonstration. — Tous les graphes lunettes sauf ceux de la figure 3.3 sont 4-transitifs par le lemme 3.7. On suppose donc le graphe 4-transitif.

Soit $(c_0, c_1, \dots, c_p)$ le cycle auquel on a adjoint le chemin $(c_0 = s_0, s_1, \dots, s_n = c_k)$, on peut supposer $n > 1$ au vu de la remarque 3.5. Son groupe de taquin est donc engendré par les cycles $\mu = (c_1\ c_2\ \dots\ c_k{=}s_n\ s_{n-1}\ \dots\ s_1)$ et $\nu = (s_1\ \dots\ s_n{=}c_k\ c_{k+1}\ \dots\ c_p)$. On a :

$$\begin{aligned}\mu\nu\mu^{-1}\nu^{-1} &= (c_1\ s_1\ \dots\ s_{n-1}\ c_{k+1}\ \dots\ c_p)\nu^{-1}\\ &= \begin{cases}(s_1\ c_1)(c_k\ c_{k+1}) & \text{si } k > 1\\ (c_1\ c_2\ s_1) & \text{si } k = 1\end{cases}\end{aligned}$$

Par 4-transitivité on obtient toutes les doubles transpositions ou tous les 3-cycles, qui engendrent $\mathfrak{A}_{S\setminus\{s_0\}}$. □

4. Structure des groupes de taquin

4.1. Décomposition en graphes doublement connexes

Définition 4.1. — Un graphe $G = (S, A)$ est *doublement connexe* si pour tout $s \in S$, le graphe induit $G[S \setminus \{s\}]$ est encore connexe et si S n'est pas réduit à un singleton.

Remarque 4.2. — Un graphe doublement connexe avec strictement plus de 2 sommets ne contient pas de sommet de degré 1.

Exemple 4.3. — Tout les graphes du tableau 3.3 sont doublement connexes. Les arbres non triviaux ne sont pas doublement connexes.

Définition 4.4. — Soit $G = (S, A)$ un graphe.

- Un sommet $s \in S$ est dit *critique* si $G[S \setminus \{s\}]$ n'est pas connexe. On note S_{crit} l'ensemble des sommets critiques.

- Soient s un sommet non critique, H le graphe induit par la composante connexe de s dans $G[S \setminus S_{crit}]$.
  Si H n'est pas réduit à un sommet, on appelle composante doublement connexe de s le sous graphe G_s (de G) induit par H auquel on ajoute ses voisins (critiques) dans G.
- On note $\mathcal{C}_G$ l'ensemble des *composantes doublement connexes.*

Exemple 4.5. —

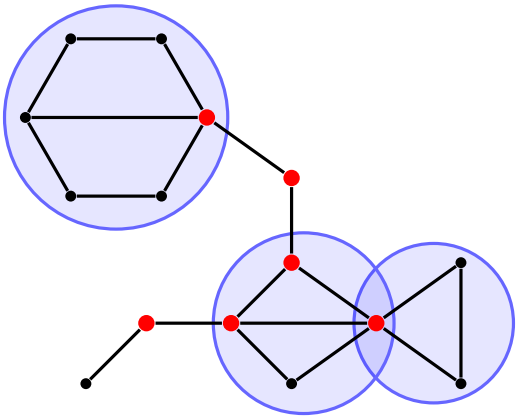


FIGURE 4. Décomposition en composantes doublement connexes

Lemme 4.6. — *Soit H un sous-graphe stricte d'un graphe G doublement connexe. Alors on peut adjoindre un chemin de G à H.*

Remarque 4.7. — En répétant cette opération, on peut donc passer de H à G par adjonctions successives de chemins.

Démonstration. — S'il existe une arête de $A_G \setminus A_H$ reliant deux sommets de H, on peut l'adjoindre. Sinon il existe un sommet $t_0 \in S_G \setminus S_H$.

On considère alors le plus court chemin qui relie t_0 à un sommet de H : $(t_0, t_1, \ldots, t_n)$ où t_n est le seul élément de H du chemin.

On considère les ensembles (disjoints) $S_H \setminus \{t_0\}$ et $\{t_0, t_1, \ldots, t_{n-1}\}$, qu'on relie par un chemin minimal dans $G[S \setminus \{t_n\}]$ (possible par double connexité) : $(t_i{=}s_0, s_1, \cdots, s_k)$ où $i < n$ et s_k est le seul sommet de H du chemin.

Alors on peut adjoindre $(t_n, t_{n-1}, \ldots, t_i{=}s_0, s_1, \ldots, s_k)$ à H. □

4.2. Groupes des graphes doublement connexes

Lemme 4.8. — *Soit G un graphe de taille au moins 4 tel que $T(G, s_0) \supseteq \mathfrak{A}_{S\setminus\{s_0\}}$ et c un chemin qu'on peut lui adjoindre. Soit $\tilde{G} = (\tilde{S}, \tilde{A})$ l'adjonction de c à G, alors $T(\tilde{G}, s_0) \supseteq \mathfrak{A}_{\tilde{S}\setminus\{s_0\}}$.*

Remarque 4.9. — Si G doublement connexe possède un sous-graphe H possédant au moins 4 sommets tel que $T(H, s_0) \supseteq \mathfrak{A}_{S_H\setminus\{s_0\}}$, alors grâce à la remarque 4.7 on a $T(G, s_0) \supseteq \mathfrak{A}_{S_G\setminus\{s_0\}}$.

Démonstration. — On note $c = (s_0, s_1, \dots, s_n)$ le chemin et on suppose que la case blanche commence en s_0.

Soit $c = (u_1\ u_2\ u_3) \in \mathfrak{S}_{\tilde{S}\setminus\{s_0\}}$ un 3-cycle.

- Il existe $\sigma \in T(\tilde{G}, s_0)$ telle que $\sigma(\{u_1, u_2, u_3\}) \subseteq S$.
  - On montre le résultat suivant : pour tout $a \neq b \in S\setminus\{s_0\}$, il existe $\rho_{a,b} \in T(\tilde{G}, s_0)$ tel que :
$$\begin{cases} \rho_{a,b}(s_i) = s_{i+1} (\forall 1 \leqslant i < n) \\ \rho_{a,b}(a),\ \rho_{a,b}(b) \in S \end{cases}$$
    Quitte à composer par $(t\ a\ b) \in T(G, s_0) \subseteq T(\tilde{G}, s_0)$ où $t \in S \setminus \{s_0, a, b\}$ (car G est de taille supérieure à 4), on peut supposer $a, b \neq s_n$.
    On considère la suite de coup $[s_0, s_1, \dots, s_n]$, par connexité on a une suite $[s_n{=}t_0, t_1, \dots, t_k{=}s_0]$ dans G. Alors $\rho_{a,b} = \langle s_0, s_1, \dots, s_n{=}t_0, t_1 \dots, t_k{=}s_0\rangle$ convient.
  - Si $u_1, u_2, u_3 \in S$ il n'y a rien à faire.
  - Si deux des trois, par exemple u_1, u_2, sont dans S, et $u_3 = s_k$ où $0 < k < n$. Alors on applique ρ_{u_1,u_2} qui amène u_3 sur s_{k-1}, puis $\rho_{\rho^{-1}_{u_1,u_2}(u_1),\rho^{-1}_{u_1,u_2}(u_2)}$ qui l'emmène sur s_{k-2} et ainsi de suite, jusqu'à l'envoyer dans S.
  - Si 0 ou 1 des u_i est dans S, on fait de même en choisissant s'il le faut des points a et b arbitraires pour se ramener au cas précédent.
- $c \in T(\tilde{G}, s_0)$. Comme $\nu = (\sigma(u_1)\ \sigma(u_2)\ \sigma(u_3)) \in T(G, s_0) \subseteq T(\tilde{G}, s_0)$, on a $c = \sigma^{-1}\nu\sigma \in T(\tilde{G}, s_0)$.

□

Théorème 4.10. — *Soit G un graphe doublement connexe, alors :*
$$T(G, s_0) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} \text{ si } G \text{ est un cycle} \\ \mathfrak{S}_5 \text{ si } G \simeq G_{ex} \\ \mathfrak{A}_n \text{ si } G \text{ est 2-coloriable} \\ \mathfrak{S}_n \text{ sinon} \end{cases}$$
où $n = |S| - 1$.

Démonstration. — Par les propositions 3.1 et 3.2, il suffit de traiter le cas où $G = (S, A)$ n'est pas un cycle et n'est pas isomorphe à G_{ex}.

- G contient un graphe lunette L. On part d'un sommet, on avance sans repasser par le sommet précédent (possible car le degré de chaque sommet est au moins 2) jusqu'à tomber sur un sommet déjà rencontré. On trouve alors un cycle puis on conclut par le lemme 4.6.
- Si $L \not\simeq G_{ex}$, alors $T(L, s_0) \supseteq \mathfrak{A}_{S_L\setminus\{s_0\}}$. Par le lemme 3.8 puis la remarque 4.9.
- Si $L \simeq G_{ex}$. On numérote les sommets de L comme dans la figure 1, et on distingue selon le chemin c qu'on obtient par le lemme 4.6 (car $G \not\simeq G_{ex}$) :
  - $c = (1$ resp. $2, x, 6$ resp. $5)$: l'adjonction de c à L est isomorphe à $\widehat{G}_{ex}$, on conclut comme précédemment.
  - $c = (3, x, 4)$: on enlève les sommets 5 et 6 et on adjoint c pour obtenir un graphe lunette non isomorphe à G_{ex}.
  - $c = (0, \dots, 1$ ou $2)$: idem en enlevant également 5 et 6.

— $c = (0, \ldots, 3$ ou 4 ou 5 ou $6)$: idem en enlevant 1 et 2.
— Sinon, idem en enlevant 0.

- $T(G, s_0) \subseteq \mathfrak{A}_{S\setminus\{s_0\}}$ si et seulement si G est 2-coloriable.
  — Si G est 2-coloriable, la case blanche change de couleur à chaque coup donc une suite de coup close correspond à un nombre pair de coups donc de transpositions.
  — Si $T(G, s_0) \subseteq \mathfrak{A}_{S\setminus\{s_0\}}$, on remarque que toute de suite coups amenant la case blanche sur un même sommet ont même signature dans $\mathfrak{S}_S$. En effet si α et β correspondent à deux suite de coups de s_0 à s_1, $\alpha\beta^{-1} \in T(G, s_0)$. On peut donc colorier chaque sommet en fonction de la signature des suites de coups amenant la case blanche de s_0 à ce sommet.

□

4.3. Produit de groupes de taquin

Lemme 4.11. — *Soient $G = (S_G, A_G)$ et $H = (S_H, A_H)$ tels que $S_G \cap S_H = \setminus\{s_0\}$, alors :*

$$T(G \cup H, s_0) \simeq T(G, s_0) \times T(H, s_0)$$

où $G \cup H = (S_G \cup S_H, A_G \cup A_H)$.

Démonstration. — On considère l'isomorphisme suivant :

$$\begin{aligned} \Phi : \ T(G, s_0) \times T(H, s_0) &\longrightarrow T(G \cup H, s_0) \\ (\mu, \nu) &\longmapsto \left(s \mapsto \begin{cases} \mu(s) & \text{si } s \in S_G \\ \nu(s) & \text{si } s \in S_H \end{cases} \right) \end{aligned}$$

- C'est un morphisme injectif.
- Il est surjectif. Soit $\langle s_0, s_1, \ldots, s_n \rangle \in T(G \cup H, s_0)$.
  On note $\{k_0{=}0 < k_1 < \ldots < k_r{=}n\} = \{0 \leqslant k \leqslant n \mid s_k = s_0\}$. On remarque que chaque $\sigma_i = \langle s_{k_i}, s_{k_i+1}, \ldots, s_{k_{i+1}} \rangle$ est dans $T(G, s_0)$ ou $T(H, s_0)$ (vu comme sous-groupes de $\mathfrak{S}_{S_G \cup S_H}$), donc :

$$\begin{aligned} \langle s_0, s_1, \ldots, s_n \rangle &= \prod_{i=0}^{r-1} \sigma_i \\ &= \Phi \left(\prod_{\substack{i=0 \\ \sigma_i \in T(G,s_0)}}^{r-1} \sigma_i \ , \prod_{\substack{i=0 \\ \sigma_i \in T(H,s_0)}}^{r-1} \sigma_i \right) \text{ car les supports sont disjoints} \end{aligned}$$

  où les produits doivent être pris dans l'ordre décroissant des i.

□

Théorème 4.12. — *Soit $G = (S, A)$ un graphe, $s_0 \in S$. Alors :*

$$T(G, s_0) \simeq \prod_{G_s \in \mathcal{C}_G} T(G_s, s)$$

Démonstration. — On procède par récurrence forte sur le nombre de sommets de G.

- Si G est doublement connexe : C'est le théorème 4.10.

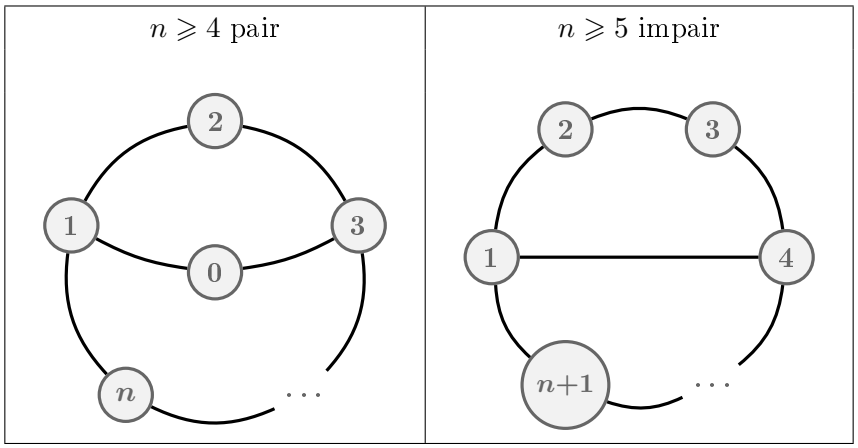
- Sinon : Soit $s_0 \in G$ un sommet critique. Soient $H_1, \dots, H_k$ (avec $k > 1$) les composantes connexes de $G[S \setminus \{s_0\}]$. On considère $G_1 = G[S_{H_1} \cup \{s_0\}]$ et $G_2 = G[S_{H_2} \cup \dots \cup S_{H_k} \cup \{s_0\}]$ deux sous-graphes strictes de G. Par le lemme 4.11, $T(G, s_0) \simeq T(G_1, s_0) \times T(G_2, s_0)$, et comme $\mathcal{C}_G = \mathcal{C}_{G_1} \sqcup \mathcal{C}_{G_2}$ on conclut par hypothèse de récurrence.

□

Corollaire 4.13. — *Les graphes de taquin sont exactement les produits finis de $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$ et $\mathfrak{A}_n$ à isomorphisme près.*

Démonstration. — Par le théorème 4.12 et le lemme 4.11, il suffit de savoir construire des graphes pour $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

- $\mathbb{Z}/n\mathbb{Z}$: Cycle à $n+1$ sommets.
- $\mathfrak{S}_n$: Graphe complet à $n+1$ sommets.
- $\mathfrak{A}_n$: Si $n \leqslant 3$, $\mathfrak{A}_n \simeq \mathbb{Z}/n\mathbb{Z}$. Sinon, les graphes lunettes suivants conviennent :



□

Exemple 4.14. —

- Les groupes abéliens sont des groupes de taquin.
- Le groupe du graphe de la figure 1 est isomorphe à $\mathfrak{A}_5 \times \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$.
- Le groupe du taquin usuel de Sam Loyd est $\mathfrak{A}_{15}$.

PARTIE II. LE TAQUIN DE CONWAY

Conway a construit un jeu similaire au taquin [**1**], où les cases sont les 13 points de $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$. On définit alors un ensemble de coups possibles, et les permutations de $\mathfrak{S}_{12}$ qu'ils engendrent se trouvent être le groupe sporadique M_{12}.

Pour démontrer cela, on utilisera les codes de Golay ternaires qui nous permettent de construire un système de Steiner $S(5, 6, 12)$.

5. Description du jeu

5.1. Système de Steiner

Commençons par une notion importante pour la description et la compréhension du jeu.

Définition 5.1. — Un Système de Steiner $S(t, k, n)$ est un ensemble Ω à n éléments, et un ensemble de sous-ensembles de Ω à k éléments (appelés blocs) tel que toute partie à t éléments de Ω est contenue dans un unique bloc.

Exemple 5.2. —

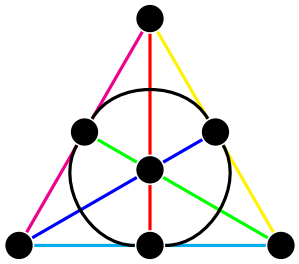


FIGURE 5. Le plan de Fano est un $S(2, 3, 7)$

On note $\mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$ le plan projectif sur $\mathbb{Z}/p\mathbb{Z}$ (où p est premier), c'est à dire les droites (sous-espaces vectoriels de dimension 1) de $(\mathbb{Z}/p\mathbb{Z})^3$.

Théorème 5.3. — *L'espace $\mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$ est un système de Steiner $S(2, p+1, p^2+p+1)$ dont les blocs sont les plan de $(\mathbb{Z}/p\mathbb{Z})^3$.*

Démonstration. — On note $\mathcal{P}$ les droites et $\mathcal{L}$ les plans (sous-espaces vectoriels de dimension 2) de $(\mathbb{Z}/p\mathbb{Z})^3$.

(1) Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ agit naturellement sur $(\mathbb{Z}/p\mathbb{Z})^3 \setminus \{0\}$ librement, il y a donc $\frac{p^3-1}{p-1} = p^2 + p + 1$ droites dans $\mathcal{P}$.
(2) Le même argument appliqué à un plan ($\simeq (\mathbb{Z}/p\mathbb{Z})^2$) montre que chaque plan de $\mathcal{L}$ contient $\frac{p^2-1}{p-1} = p + 1$ droites.
(3) Toute paire de droites distinctes engendre un unique plan.

□

Remarque 5.4. — L'ensemble des formes linéaires non nulles de $(\mathbb{Z}/p\mathbb{Z})^3$ quotienté par $(\mathbb{Z}/p\mathbb{Z})^\times$ s'identifie aux plans de $(\mathbb{Z}/p\mathbb{Z})^3$, donc il y a également p^2+p+1 plans.

On s'intéresse dans la suite au cas $p=3$. Le plan projectif forme un $S(2,4,13)$, illustré sur la figure 6. On appelle $\mathcal{P}$ les points (donc les droites) du plan projectif et $\mathcal{L}$ les lignes (donc les plans). Il sera souvent pratique d'identifier les points à des numéros comme sur la figure.

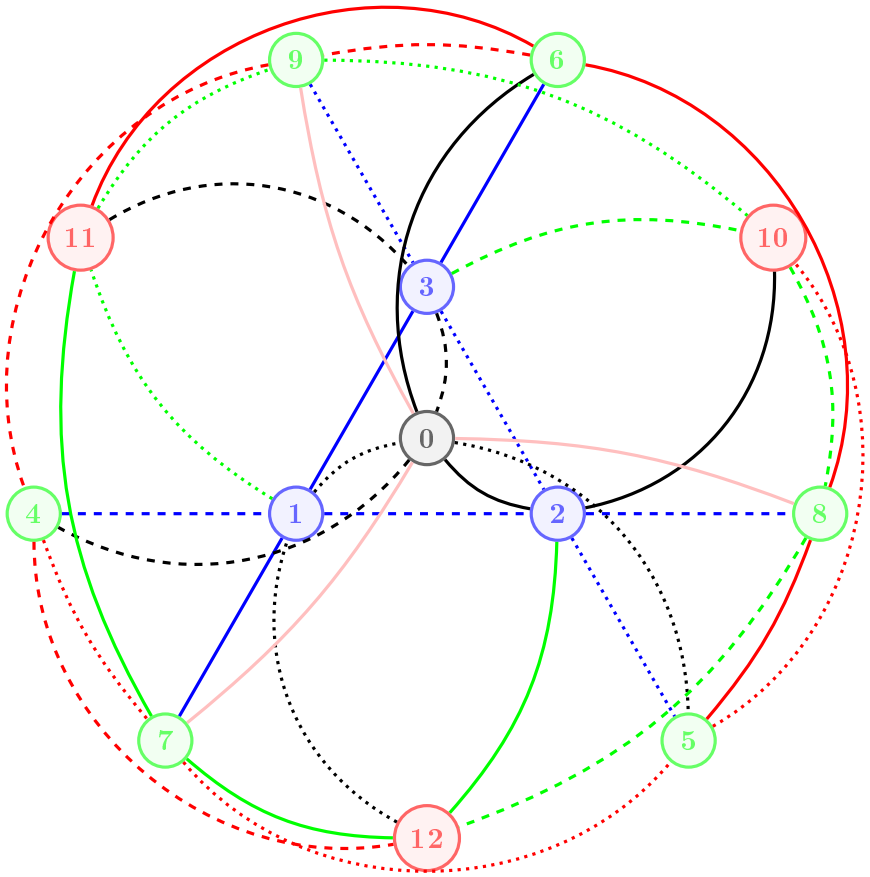


FIGURE 6. Système de Steiner $S(2,4,13)$

Quelques propriétés utiles pour la suite :

Proposition 5.5. — *Les propriétés suivantes sont satisfaites :*

(*a*) *On a* $|\mathcal{L}|=13$.
(*b*) *Par un point de* $\mathcal{P}$ *passe exactement* 4 *lignes de* $\mathcal{L}$.
(*c*) *Deux lignes distinctes de* $\mathcal{L}$ *s'intersectent en un unique point de* $\mathcal{P}$.
(*d*) *Tout ensemble de points* $\mathcal{O}\subseteq\mathcal{P}$ *tel que* 3 *points n'appartiennent jamais à une même ligne (on appellera cela un ovale) est de cardinal au plus* 4.

Démonstration. —

(*a*) $|\mathcal{L}| = \dfrac{\binom{13}{2}}{\binom{4}{2}} = 13$

(*b*) $\dfrac{13-1}{4-1} = 4$

(*c*) Fixons une ligne ℓ, par (*b*) il y a $4 \times (4-1) = 12$ autres lignes l'intersectant, donc toutes les lignes la rencontrent par (*a*).

(*d*) Si $\mathcal{O}$ contient plus de 4 points, prenons 3 de ses points : $1, 2, 3$. En considérant les 3 lignes passant par deux de ces points, comme il existe une unique ligne passant par deux points, on obtient 6 nouveaux points n'appartenant pas à l'ovale : $4, 5, 6, 7, 8, 9$ (figure 7). On prend un nouveau point dans l'ovale : 0. En considérant les 3 lignes $\overline{01}, \overline{02}, \overline{03}$ on obtient au moins 3 nouveaux points (par exemple la ligne $\overline{01}$ ne peut qu'intersecter la ligne $\overline{23}$) : les points $10, 11, 12$ (figure 8). On a donc atteint tous les points de $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$: 4 dans l'ovale et 9 à l'extérieur.

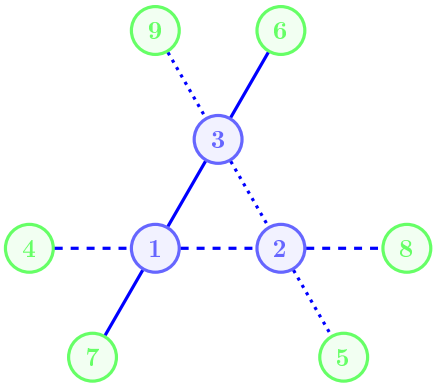


FIGURE 7

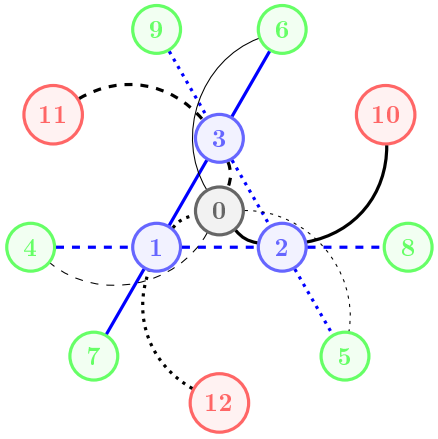


FIGURE 8

□

Remarque 5.6. — En construisant un ovale contenant 4 points et en s'inspirant de la preuve de (*d*), on peut montrer l'unicité (à isomorphisme près) de $S(2, 4, 13)$.

5.2. Le taquin de Conway

Le jeu de Conway est très similaire à celui du taquin étudié en première partie. Initialement, on place sur les points (ou cases) du plan projectif $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$ des jetons numérotés de 1 à 12 (comme sur la figure), sauf sur le point 0. La case sans jeton est appelée la *case blanche* (en 0 initialement). On définit un coup $[p, q]$ comme suit. Supposons que la case blanche soit au point p, et que $l = \{p, q, r, s\}$ est l'unique ligne de $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$ passant par p et q. Alors le coup $[p, q]$ consisté à bouger le jeton de q en p et à échanger les jetons en r et s. Ce coup emmène donc la case blanche de p vers q. Le prochain coup devra donc être de la forme $[q, \cdot]$.

Un coup $[p, q]$ induit la permutation $\langle p, q\rangle = (p\ q)(r\ s) \in \mathfrak{S}_{\mathcal{P}} \simeq \mathfrak{S}_{13}$.

Une suite de coups $[p_0, p_1]$, $[p_1, p_2]$, ... $[p_{n-1}, p_n]$ qu'on notera $[p_0, p_1, \dots, p_n]$ correspond donc à la permutation $\langle p_0, p_1, \dots, p_n\rangle = \langle p_{n-1}, p_n\rangle \circ \cdots \circ \langle p_0, p_1\rangle$.

Une suite de coups débutant et terminant en 0 est dite close.

On note $G \subseteq \mathfrak{S}_{\mathcal{P}\setminus\{0\}} \simeq \mathfrak{S}_{12}$ l'ensemble des permutations correspondant à une suite de coup close. Il forme manifestement un sous-groupe de $\mathfrak{S}_{12}$.

Nous allons montrer dans la suite que G est isomorphe au groupe de Mathieu M_{12}. Un bon début serait donc de définir M_{12} !

6. Le groupe de Mathieu M_{12}

6.1. Définition

Définition 6.1. — On définit M_{12} comme le sous-groupe de $\mathfrak{S}_{12}$ stabilisant les blocs d'un système de Steiner $S(5, 6, 12)$.

Pour que cette définition ait dû sens il faut qu'un tel système existe et qu'ils soit unique à isomorphisme près. C'est l'objectif de la dernière partie.

Remarque 6.2. — On se donnera le mal de reprouver ces deux faits pour épargner le lecteur de la définition suivante : M_{12} est le sous-groupe de $\mathfrak{S}_{12}$ engendré par (3 4)(6 7)(9 10)(11 12) et (1 2 3)(4 5 6)(7 8 9)(10 11 12).

Nous aurons également besoin du résultat suivant (démontré dans la dernière partie) :

Proposition 6.3. — *Le groupe M_{12} agit exactement 5-transitivement sur les 12 éléments.*

On en déduit en particulier que $|M_{12}| = 12 \times 11 \times 10 \times 9 \times 8 = 95040$.

6.2. Code de Golay ternaire

Cette section donne une manière de constructrice un système de Steiner $S(5, 6, 12)$ à partir d'un code de Golay.

Définition 6.4. — Soit $v = (v_x)_{x\in X}$ un vecteur de $(\mathbb{Z}/p\mathbb{Z})^X$.

- On appelle support de v l'ensemble $\mathrm{Supp}(v) = \{x \in X \mid v_x \neq 0\}$.
- On appelle poids $wt(v) = |\mathrm{Supp}(v)|$ le cardinal du support de v.

Définition 6.5. — Un *code de Golay ternaire* est un sous-espace vectoriel de $(\mathbb{Z}/3\mathbb{Z})^{12}$ de dimension supérieure ou égale à 6 dont les vecteurs non nuls sont de poids au moins 6.

Théorème 6.6. — *Les supports des éléments de poids 6 d'un code de Golay $\mathcal{C}$ forment un système de Steiner $S(5, 6, 12)$.*

Démonstration. — Notons $\mathcal{S} = \{\mathrm{Supp}(v) \mid v \in \mathcal{C}, wt(v) = 6\}$ les supports des éléments de poids 6.

Soit X un sous-ensemble de $[\![1, 12]\!]$. On veut montrer qu'il existe un unique $A \in \mathcal{S}$ tel que $X \subseteq A$.

- Unicité : Soit v, w de poids 6 dans $\mathcal{C}$ dont les supports contiennent X. On considère $I = \{i \in X \mid v_i = w_i\}$.
  - Si $|I| \geqslant 3$, alors $\mathrm{Supp}(v - w) = \mathrm{Supp}(v) \cup \mathrm{Supp}(w) \setminus I$ est de cardinal inférieur à 5 donc $v - w = 0$ d'où $\mathrm{Supp}(v) = \mathrm{Supp}(w)$.

– SI $X \setminus I = \{i \in X \mid v_i = -w_i\}$ est de cardinal supérieur à 3 donc, $v + w = 0$ (même argument) puis $\mathrm{Supp}(v) = \mathrm{Supp}(w)$.

• Existence : Soit $Q = {(\mathbb{Z}/3\mathbb{Z})^{12}}/{\mathcal{C}}$ l'espace quotient, il est de dimension inférieure à 6 donc $|Q| \leqslant 3^6$. Fixons $\omega \in [\![1, 12]\!]$.

On note e_i le i-ème vecteur de la base canonique. On considère les vecteurs suivants :

(0) Le vecteur nul 0 (il y en a 1).
(1) Les vecteurs $\pm e_i$ pour $1 \leqslant i \leqslant 12$ (il y en a $2 \cdot 12 = 24$).
(2) Les $\pm e_i \pm e_j$ pour $1 \leqslant i < j \leqslant 12$ ($4 \cdot \binom{12}{2} = 264$).
(3) Les $\pm e_\omega \pm e_i \pm e_j$ pour $1 \leqslant i < j \leqslant 12$ différents de ω ($8 \cdot \binom{11}{2} = 440$).

Ces éléments sont manifestement dans des classes d'équivalence différentes (car la différence de deux tels éléments est de poids inférieur à 5). On en a trouvé $1+24+264+440 = 729 = 3^6$! Donc $|Q| = 3^6$, $\mathcal{C}$ est en fait de dimension exactement 6 et on a trouvé un système de représentants de Q.

Comme ω est quelconque, on peut supposer que $X = \{\omega, x, y, z, t\}$. On considère l'ensemble $V = \{e_x \pm e_y \pm e_z\}$ de cardinal 4. Tout $v \in V$ est dans la classe d'un r_v de la liste précédente. En regardant le support de $v - r_v \in \mathcal{C}$, on peut écrire $\mathrm{Supp}(r_v) = \{\omega, r_v^1, r_v^2\}$ (de type (3)) avec r_v^1, r_v^2 différents de x, y, z, ω. Les r_v sont tous distincts car $wt(v - w) \leqslant 2$ pour $v, w \in V$. Les r_v^i sont tous distincts car si $r_v^i = r_w^j$, alors $v - r_v$ et $w - r_w$ sont deux vecteur de $\mathcal{C}$ de poids 6 dont le support contient $\{\omega, x, y, z, r_v^i\}$, donc par unicité (ci-dessus) $v - r_v = \pm(w - r_w)$. Or la coordonnée x de ces deux vecteurs est 1, donc $v - r_v = w - r_w$ puis $v = w$ (car les supports de v et r_v sont disjoints).

En d'autres mots, $\phi : (v, i) \in V \times \{1, 2\} \longmapsto r_v^i \in [\![1, 12]\!] \setminus \{\omega, x, y, z\}$ est injective, puis surjective par égalité des cardinaux. On trouve donc $v \in V$ tel que $t \in \mathrm{Supp}(r_v)$, on a donc $X \subset \mathrm{Supp}(v - r_v)$ avec $v - r_v \in \mathcal{C}$ de poids 6 !

□

7. Le groupe G est isomorphe à M_{12}

7.1. À la recherche du code de Golay

On cherche à faire agir G sur un certain code de Golay de façon à stabiliser les supports des vecteurs. Les coups du taquin ont une interprétation intuitive dans $(\mathbb{Z}/3\mathbb{Z})^{\mathcal{P}} \simeq (\mathbb{Z}/3\mathbb{Z})^{13}$, mais cet espace est de dimension 13. Cependant G correspond aux séquences de coups qui ne font pas bouger la case 0, on pourra donc plus-tard oublier cette coordonnée pour retrouver un espace de dimension 12.

Comme un coup sur le taquin ne fait qu'intervenir les cases d'une même ligne, on peut s'intéresser à l'espace :

$$\mathcal{C} = \mathrm{Vect}(h_\ell \mid \ell \in \mathcal{L}) \quad \text{où} \quad h_\ell = \sum_{x \in \ell} e_x \quad \text{représente une ligne}$$

On prend aussi $\mathcal{C}' = \left\{ c \in \mathcal{C} \mid \sum_{p\in\mathcal{P}} c_p = 0 \right\}$.
Il se produit en fait une série de miracles :

Proposition 7.1. — *Soient $c, d \in \mathcal{C}$, alors :*

(1) $\sum_{p\in\mathcal{P}} c_p d_p = \left(\sum_{p\in\mathcal{P}} c_p\right)\left(\sum_{p\in\mathcal{P}} d_p\right)$
(2) $wt(c) \equiv 0$ *ou* $1\,[3]$
(3) $c \in \mathcal{C}'$ *ssi* $wt(c) \equiv 0\,[3]$
(4) *Pour tout* $\ell \in \mathcal{L}$, $\sum_{p\in\mathcal{P}} c_p = \sum_{p\in\ell} c_p$
(5) $\mathcal{C}'$ *est l'orthogonal de* $\mathcal{C}$ *(pour le produit scalaire définit ci-dessous)*
(6) $\dim(\mathcal{C}) = 7$ *et* $\dim(\mathcal{C}') = 6$
(7) *Le poids minimal des vecteurs non nuls de* $\mathcal{C}$ *(resp.* $\mathcal{C}'$*) est* 4 *(resp.* 6*), et les vecteurs de poids* 4 *sont exactement les* $\pm h_\ell$*.*

Le produit scalaire considéré (qui est bilinéaire symétrique) est :

$$c \cdot d = \sum_{p\in\mathcal{P}} c_p d_p$$

Démonstration. —
(1) Par bilinéarité de la formule, il suffit de le montrer pour les lignes ce qui est manifestement vrai (car l'intersection de deux lignes est un point ou la ligne complète comme c'est un système de Steiner $S(2,4,13)$).
(2) $wt(c) \equiv \sum_{p\in\mathcal{P}} c_p^2 = \left(\sum_{p\in\mathcal{P}} c_p\right)^2$ $[3]$
(3) Par définition de $\mathcal{C}'$ en utilisant (1) et (2).
(4) On applique (1) à h_ℓ et c.
(5) On a déjà $\mathcal{C}' \subseteq \mathcal{C}^\perp$ par (1). Montrons $(\mathcal{C}')^\perp \subseteq \mathcal{C}$, soit $v \in (\mathcal{C}')^\perp$.
   - On se ramène au cas au Supp(v) ne contient jamais 3 points d'une même ligne (cela s'appelle un ovale). Si 3 points du support sont sur une même ligne ℓ, on peut ajouter $\pm h_\ell$ pour réduire strictement le poids de v en restant dans $(\mathcal{C}')^\perp$. On itère le processus jusqu'à tomber sur un ovale.
   - v est nul. On suppose par l'absurde $wt(v) > 0$ donc $1 \leqslant wt(v) \leqslant 4$ par la propriété (d). Il existe une ligne ℓ disjointe de Supp(v). En effet par 4 points il passe $4 \times 4 - \binom{4}{2} = 10$ lignes (propriétés (b) et (c)). On prend donc une des (au moins) 3 lignes restantes (figure 3). On fixe un point de l'ovale, il existe une ligne k passant par ce point mais aucun autre de l'ovale par la propriété (b). Alors $h_l - h_k \in \mathcal{C}'$ mais est de produit scalaire avec v non nul, c'est absurde.

   Cela signifie que $v \in \mathcal{C}$.
(6) $\dim(\mathcal{C}) + \dim(\mathcal{C}') = 13$ et $dim(\mathcal{C}') = dim(\mathcal{C}) - 1$

(7) On sait déjà que le poids minimal est moins que 4. Par (2), le poids 2 est impossible. Soit v de poids minimal.
- v n'est pas de poids 1 : Sinon on prend ℓ ne rencontrant pas le point du support, alors par (1) et (4) :
$$wt(c) \equiv \left(\sum_{p\in\mathcal{P}} c_p\right)^2 = \left(\sum_{p\in\ell} c_p\right)^2 = 0\,[3]$$
- v n'est pas de poids 3 : On prend ℓ passant par un seul des 3 points du support, puis on conclut par le même argument.
- $v = \pm h_\ell$: Par l'absurde, supposons que $\mathrm{Supp}(v)$ n'est pas sur une ligne. Alors si v possède 3 éléments sur une même ligne ℓ, quitte à ajouter $\pm h_\ell$ ont fait diminuer strictement $wt(v)$ ce qui est absurde. Donc $\mathrm{Supp}(v)$ est un ovale, comme dans (5) on prend ℓ qui n'intersecte pas $\mathrm{Supp}(v)$ et on conclut comme les points précédents.

On déduit par (3) que le poids minimal dans $\mathcal{C}'$ est au moins 6, qui est atteint par $h_\ell - h_k$ avec $\ell \neq k$ (propriété (c)).

□

***Remarque 7.2* (Une autre preuve de (5) et (6)).** —
Comme $\dim(\mathcal{C}') = \dim(\mathcal{C}) - 1$ et $C' \subseteq \mathcal{C}^\perp$, on a :
$$13 = \dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) \geqslant 2\dim(\mathcal{C}) - 1$$
donc $\dim(\mathcal{C}) \leqslant 7$. On trouve 7 vecteurs linéairement indépendants en prenant les h_ℓ associés aux lignes $\overline{01}, \overline{02}, \overline{03}$ (noires), $\overline{47}, \overline{58}, \overline{69}$ (rouges) et $\overline{07}$ (beige). Voici la matrice représentant ces lignes (les colonnes) pour se convaincre de l'indépendance :

$$\begin{bmatrix}
\bullet & \bullet & \bullet & \circ & \circ & \circ & \bullet \\
\bullet & \circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \bullet & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \bullet & \circ & \circ & \circ & \circ \\
\circ & \circ & \bullet & \bullet & \circ & \bullet & \circ \\
\bullet & \circ & \circ & \bullet & \bullet & \circ & \circ \\
\circ & \bullet & \circ & \circ & \bullet & \bullet & \circ \\
\circ & \circ & \circ & \bullet & \circ & \circ & \bullet \\
\circ & \circ & \circ & \circ & \bullet & \circ & \bullet \\
\circ & \circ & \circ & \circ & \circ & \bullet & \bullet \\
\circ & \bullet & \circ & \bullet & \circ & \circ & \circ \\
\circ & \circ & \bullet & \circ & \bullet & \circ & \circ \\
\bullet & \circ & \circ & \circ & \circ & \bullet & \circ
\end{bmatrix}$$

D'où (5) par égalité des dimensions.

On aimerait croire que $\mathcal{C}'$ est un code de Golay, mais il vit en dimension 13. On y est presque !

7.2. À la recherche de l'action taquine

On cherche maintenant une action qui stabilise $\mathcal{C}$. Malheureusement l'action naturelle (qui consiste à permuter les coordonnées) n'a aucune raison de stabiliser $\mathcal{C}$.

Pour rester dans $\mathcal{C}$ et imiter l'action naturelle sur la coordonnée p ($([p,q]\bullet v)_p = v_q$), on pose $[p,q]\bullet v = v + (v_q - v_p)h_\ell$, où $\ell = \{p,q,r,s\}$ est la ligne passant par p et q. Avec $[p,q]\bullet v = w$ on a donc :

$$\begin{cases} w_p = v_q \qquad \text{(On a tout fait pour !)} \\ w_q = -v_q - v_p \\ w_r = v_r + v_q - v_p \\ w_s = v_s + v_q - v_p \\ w_i = v_i \qquad \text{pour les autres coordonnées} \end{cases}$$

Quitte à se placer sur un sous-espace de $\mathcal{C}$ (si possible de dimension 6), on aimerait de plus avoir des relations du type :

$$\begin{cases} w_q = \pm v_p \\ w_r = \pm v_s \\ w_s = \pm v_r \end{cases}$$

pour garder le même comportement sur les supports que l'action naturelle. Ceci est trop restrictif car si les trois relations étaient indépendantes on obtiendrait au mieux un espace de dimension 4. On peut alors remarquer qu'on ne s'intéressera qu'aux suites de coups closes, la coordonnée q qui correspond à la case blanche pourra donc être oubliée. Pour lier les deux équations d'après on met les mêmes signes, et la seule action non triviale qu'on obtient est :

$$\begin{cases} w_r = v_r + v_q - v_p = -v_s \\ w_s = v_s + v_q - v_p = -v_r \end{cases}$$

Pour que ces relations soient vérifiées, il faut donc se placer dans :

$$\begin{aligned} \mathcal{C}_p &= \left\{ v \in \mathcal{C} \mid \sum_{x \in \ell} v_x = -v_p \right\} \\ &= \left\{ v \in \mathcal{C} \mid \sum_{x \in \mathcal{P}} v_x = -v_p \right\} \text{ par la propriété (4)} \end{aligned}$$

On étend l'action à une suite de coups en posant :

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

Proposition 7.3. — $[p, q] \bullet \mathcal{C}_p = \mathcal{C}_q$

Démonstration. — Il suffit de vérifier que $[p, q] \bullet \mathcal{C}_p \subseteq C_q$ car $[q, p] \bullet [p, q] \bullet v = v$ par définition de l'action.

Soit $w = [p, q] \bullet v = v + (v_p - v_q)h_\ell \in [p, q] \bullet \mathcal{C}_p$ donc manifestement $w \in \mathcal{C}$, et :

$$\begin{aligned} \sum_{x \in \mathcal{P}} w_x &= w_p + w_q + w_r + w_s \text{ propriété (4)} \\ &= 4(v_q - v_p) + v_p + v_q + v_r + v_s \\ &= v_q - v_p - v_p = v_q + v_p \\ &= -w_q \end{aligned}$$

□

7.3. Le code retrouvé

On considère les suites de coups closes qui stabilisent donc $\mathcal{C}_0$. Dans ce cas, l'action agit au signe près comme l'action naturelle lorsqu'on omet la première coordonnée. Autrement dit :

Définition 7.4. — Le sous-espace vectoriel $\mathcal{G}_0 \subseteq (\mathbb{Z}/3\mathbb{Z})^{12}$ est obtenu à partir de $\mathcal{C}_0$ en oubliant la coordonnée 0, c'est donc l'image de $\mathcal{C}_0$ par l'isomorphisme :

$$\pi : (c_0, c_1, \ldots, c_{12}) \in \mathcal{C}_0 \longmapsto (c_1, \ldots, c_{12}) \in \mathcal{G}_0$$

Une suite de coups close $[p_0, p_1, \ldots, p_n]$ (où $p_0 = p_n = 0$) induit alors une permutation dans $\mathfrak{S}_{12}$ (en se restreignant à $\mathcal{P} \setminus \{0\}$), on la notera $\overline{\langle p_0, p_1, \ldots, p_n \rangle}$. On peut également transporter l'action $\bullet$ par $[p_0, p_1, \ldots, p_n] \bullet v = \pi([p_0, p_1, \ldots, p_n] \bullet \pi^{-1}(v))$.

Proposition 7.5. — *Pour tout* $\overline{\langle p_0, p_1, \ldots, p_n \rangle} \in G \subseteq \mathfrak{S}_{12}$ *et* $v \in \mathcal{G}_0$ *:*

$$\mathrm{Supp}([p_0, p_1, \ldots, p_n] \bullet v) = \overline{\langle p_0, p_1, \ldots, p_n \rangle}(\mathrm{Supp}\, v)$$

Démonstration. — Par récurrence immédiate (sur n), avec la définition de $\bullet$ on a :

$$\forall v \in \mathcal{C}_0, \mathrm{Supp}([p_0, p_1, \ldots, p_n] \bullet v) \setminus \{p_n\} = \langle p_0, p_1, \ldots, p_n \rangle(\mathrm{Supp}(v) \setminus \{p_0\})$$

□

Pour montrer que G est inclus dans M_{12}, par le théorème 6.6 il suffit maintenant de montrer que $\mathcal{G}_0$ est un code de Golay, car on aura donc que G stabilise le système de Steiner induit par $\mathcal{G}_0$, puis $G \subsetneq M_{12}$!

Proposition 7.6. — *$\mathcal{G}_0$ est un code de Golay.*

Démonstration. — On sait déjà que $\dim(\mathcal{G}_0) = \dim(\mathcal{C}_0) = 6$ (propriété (6)).

Soit $v \in \mathcal{C}_0$.

- $\underline{wt(\pi(v)) \equiv 0\,[3]\,:}$

$$\begin{aligned} wt(\pi(v)) &\equiv \sum_{p \neq 0} v_p^2 \ [3] \\ &= \sum_{p \in \mathcal{P}} v_p^2 - v_0^2 = \left(\sum_{p \in \mathcal{P}} v_p \right)^2 - v_0^2 \ \text{ par propriété (1)} \\ &\equiv 0\,[3] \ \text{ par définition de } \mathcal{C}_0 \end{aligned}$$

- $\underline{wt(\pi(v)) \neq 3\,:}$
  Par l'absurde, on aurait par la propriété (7) $wt(v) = 4$ et $v_0 \neq 0$, puis $v = \pm h_\ell$ ce qui empêche d'avoir $v_0 = -\sum_{p \in \mathcal{P}} v_p$ ($1 \not\equiv -4\,[3]$).

□

7.4. La dernière inclusion

Pour finir, il nous faut trouver des générateurs de M_{12}. Pour cela nous avons écrit un programme (Ocaml) pour générer les permutations de G, le tableau 1 résume les résultats obtenus (avec la numérotation des points de $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$ correspondante la figure 6).

Type	**Nombre**	**Exemple de permutation**	Permet de montrer
1^{12}	1	id	
1 11	17280	$\langle 0\ 10\ 7\ 9\ 12\ 11\ 0\rangle =$ $(2\ 3\ 4\ 5\ 6\ 7\ 10\ 8\ 11\ 12\ 9)$	2 transitif
$1^2\ 5^2$	9504	$\langle 0\ 6\ 12\ 7\ 11\ 0\rangle =$ $(3\ 4\ 5\ 8\ 9)\ (6\ 7\ 12\ 11\ 10)$	3 transitif
$1^2\ 2\ 8$	11880	$\langle 0\ 7\ 3\ 10\ 1\ 6\ 11\ 0\rangle =$ $(3\ 4)\ (5\ 8\ 6\ 10\ 7\ 11\ 9\ 12)$	
$1^3\ 3^3$	1760	$\langle 0\ 8\ 5\ 4\ 9\ 0\rangle =$ $(4\ 5\ 7)\ (6\ 11\ 12)\ (8\ 9\ 10)$	4 transitif
$1^4\ 4$	2970	$\langle 0\ 8\ 11\ 4\ 10\ 3\ 0\rangle =$ $(5\ 6\ 7\ 9)\ (8\ 10\ 11\ 12)$	
4 8	11880	$\langle 0\ 12\ 11\ 6\ 1\ 4\ 7\ 0\rangle =$ $(1\ 2\ 3\ 4)\ (5\ 6\ 11\ 12\ 7\ 9\ 8\ 10)$	Transitif sur les parties à 5 éléments
$1^4\ 2^4$	495	$\langle 0\ 6\ 11\ 2\ 0\rangle =$ $(2\ 6)\ (5\ 8)\ (7\ 12)\ (10\ 11)$	5 transitif avec $1^2\ 5^2$ (et la partie $\{3,4,5,8,9\}$)
6^2	7920	$\langle 0\ 7\ 10\ 9\ 4\ 2\ 11\ 0\rangle =$ $(1\ 2\ 3\ 4\ 5\ 9)\ (6\ 7\ 11\ 8\ 10\ 12)$	
3^4	2640	$\langle 0\ 9\ 3\ 6\ 2\ 7\ 10\ 11\ 0\rangle =$ $(1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8\ 9)\ (10\ 11\ 12)$	
2 10	9504	$\langle 0\ 4\ 12\ 2\ 1\ 10\ 5\ 0\rangle =$ $(1\ 2)\ (3\ 4\ 5\ 10\ 12\ 8\ 7\ 9\ 6\ 11)$	
$2^2\ 4^2$	2970	$\langle 0\ 4\ 10\ 3\ 1\ 2\ 3\ 0\rangle =$ $(1\ 2)\ (3\ 4)\ (5\ 6\ 7\ 9)\ (8\ 12\ 11\ 10)$	
2^6	396	$\langle 0\ 11\ 6\ 3\ 12\ 11\ 1\ 7\ 0\rangle =$ $(1\ 2)\ (3\ 4)\ (5\ 8)\ (6\ 12)\ (7\ 11)\ (9\ 10)$	
1 2 3 6	15840	$\langle 0\ 1\ 11\ 6\ 12\ 5\ 9\ 0\rangle =$ $(2\ 3)\ (4\ 5\ 6\ 11\ 9\ 10)\ (7\ 8\ 12)$	
Total	**95040**	Toutes les permutations peuvent être formées en moins de 9 coups.	

TABLE 1. Permutations de G générées informatiquement

Théorème 7.7. — *Le groupe G est isomorphe à M_{12}.*

Démonstration. — La partie d'avant montre que $G \subsetneq M_{12}$, il suffit maintenant de montrer que G contient suffisamment d'éléments. On va pour cela utiliser la propriété 6.3 restreignant le nombre d'éléments de M_{12}.

On peut simplement conclure par cardinalité en remarquant que notre programme à trouvé le bon nombre d'éléments.

On peut également remarquer que G agit :

- Transitivement : Il suffit de considérer par exemple les permutations de type 1 11 et 6^2 du tableau.
- 2-transitivement : En considérant la permutation de type 1 11 (du tableau), on voit que le stabilisateur de 1 agit transitivement sur les 11 autres points.
- 3-transitivement : De même, avec les permutations de type 1^2 5^2 et 1^2 2 8, le stabilisateur de 1 et 2 agit transitivement sur les 10 autres points.
- 4-transitivement : Idem avec les permutation de type 1^3 3^3 et 1^4 4 dans le stabilisateur de 1, 2 et 3.
- Transitivement sur les parties à 5 éléments : La 4 transitivité nous permet de trouver un éléments de G envoyant $(x_1, \dots x_4)$ sur $(1, \dots, 4)$ puis avec la permutation de type 4 8, on peut envoyer $\{x_1, \dots x_5\}$ sur $\{1, \dots, 5\}$.
- 5-transitivement : Les permutations de type 1^2 5^2 et 1^4 2^4 (du tableau) montrent que stabilisateur de $\{3, 4, 5, 8, 9\}$ agit 5-transitivement sur ces 5 points (car un 5-cycle et une transposition engendrent $\mathfrak{S}_5$).

Or M_{12} agit exactement 5-transitivement (propriété 6.3), d'où la dernière inclusion. □

PARTIE III. CONSTRUCTION ET UNICITÉ DE M_{12}

Cette partie a pour objectif de donner une construction d'un système de Steiner $S(5,6,12)$ et d'en démontrer l'unicité (à isomorphisme près). Cette construction est due à Cameron d'après Higman [**2**]. On commence par construire un automorphisme extérieur de $\mathfrak{S}_6$ qui nous permettra d'expliciter un système de Steiner $S(5,6,12)$. Bien que les concepts abordés soient simples, cette partie est un assez acrobatique !

8. L'automorphisme extérieur de $\mathfrak{S}_6$

8.1. Définitions

Soit A un ensemble à 6 éléments.

- Une duade de A est un sous-ensemble à 2 éléments de A. Il y en a $\binom{6}{2} = 15$.
- Une synthème de A est une partition de A en 3 duades. Il y en a $\frac{1}{3!}\binom{6}{2}\binom{4}{2}\binom{2}{2} = 15$ également.
- Un repère de A est une partition des 15 duades de A en 5 synthèmes.

Comptons le nombre de repères :

∗ Pour une synthème fixée, il y a exactement $4 \times 2 = 8$ synthèmes disjointes de la première. On dira que deux synthèmes de A sont incompatibles si elles ne sont pas disjointes.

∗ Deux synthèmes disjointes forment ensemble un cycle hamiltonien. En disposant correctement les éléments de A, on peut les représenter comme sur la figure 9.

∗ Il y a alors 4 synthèmes disjointes des 2 premières : 3 obtenues par rotation de la synthème (a) et 1 comme celle de (b). On remarque que les 3 synthèmes de type (a) sont disjointes tandis que celle de type (b) n'est compatible avec aucune autre synthème disjointe des 2 premières.

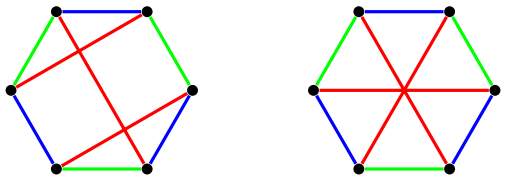


FIGURE 9. En rouge, la synthème de type (a) à gauche et de type (b) à droite.

Ainsi, 2 synthèmes disjointes déterminent entièrement un repère, il y a donc exactement $\frac{15\times 8}{5\times 4} = 6$ repères. On note X l'ensemble des repères de A.

8.2. Équivalence entre A et les repères de X

On montre ici une séries de correspondances importantes (figure 10).

- Les synthèmes de A sont des duades de X :

  En effet, si S est une synthème de A, il existe exactement $\frac{8}{5-1} = 2$ repères contenant S. Donc une synthème de A correspond à une synthème de X.

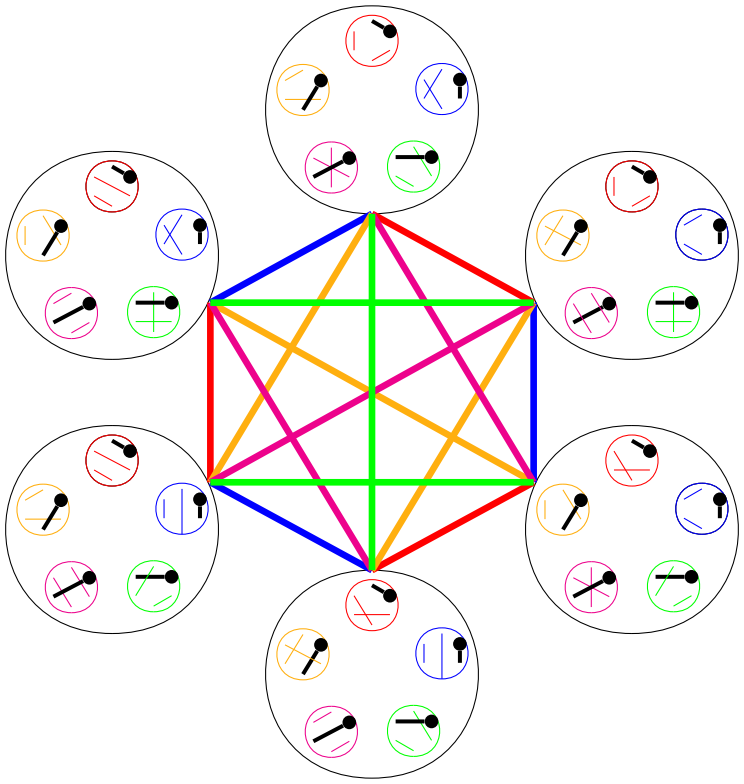


FIGURE 10. Repère de X associé à un point de A (en noir)

De plus, chaque synthème correspond à une duade de X différente (car 2 synthèmes déterminent entièrement un repère). Par cardinalité, on en déduit que les synthèmes de A sont en bijection naturelle avec les duades de X.

- Les duades de A sont les synthèmes de X :

  Si D est une duade de A, il existe exactement $\frac{1}{2!}\binom{4}{2} = 3$ synthèmes contenant D. Chacune de ces synthèmes correspondent à une duade de X ; et ces 3 duades de X forment une synthème de X. En effet, les 3 synthèmes (de A) sont différentes et incompatibles car elles contiennent toutes D, donc les 6 repères qu'elles engendrent sont disjoints.

  Toutes les duades de A correspondent de plus à des synthèmes de X différentes car les 3 synthèmes (de A) contenant les duades sont différentes (donc les duades de X associées également). Par cardinalité, on a à nouveau une bijection naturelle entre les duades de A et les synthèmes de X.

- Les éléments de A sont les repères de X :

  Si $a \in A$, il existe exactement 5 duades contenant a, et chacune de ces duades correspond à un synthème de X. Ces 5 synthèmes forment un repère de X car si D est une duade de X, elle correspond à une synthème S de A (l'intersection des deux éléments de D) et il suffit alors de considérer la duade de S contenant a.

  Tous les éléments de A correspondent à des repères de X différents car ils donnent 5 duades de X différentes (une seule sera commune pour deux éléments de A), donc

les synthèmes dans X correspondantes le seront également. Les points de A sont donc en bijection "naturelle" avec les repères de X.

On peut résumer ce qui a été dis dans la figure 11.

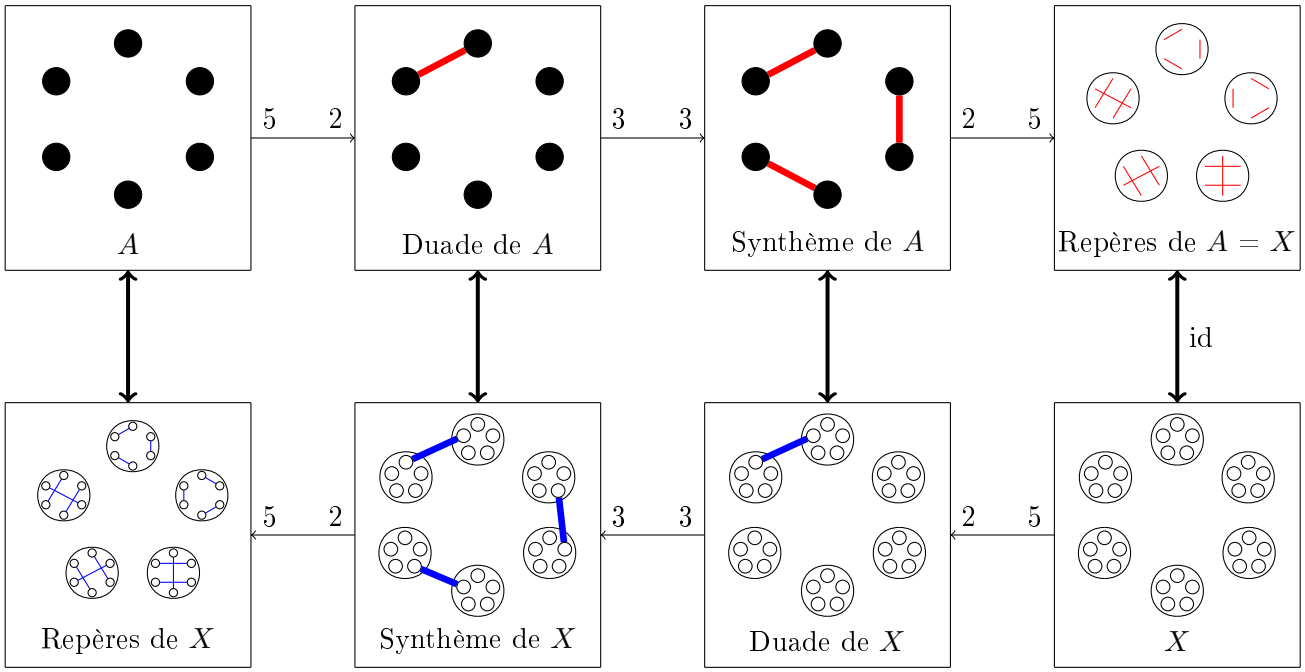


FIGURE 11. Correspondances entre A et X

Sur cette figure, les nombres à sous les flèches représentent les degrés entrants et sortants des sommets du graphe où

* Les sommets sont les éléments, les duades, les synthèmes et les repères de A (resp. X pour le graphe du bas).
* Les arrêtes $x \to y$ signifient $x \in y$.

Les bijections considérées font alors "commuter" tous les diagrammes, autrement dit, via les bijections, passer du graphe de A au graphe de X revient seulement à "inverser le sens des arêtes".

Une dernière correspondance sera utile pour la suite.

- La correspondance entre les $3+3$ partitions de A et les $3+3$ partitions de X.

  Soit $A = T \sqcup U$ une $3+3$ partition de A.

  On considère les duades de X associées aux synthèmes de A ayant une duade dans T (et donc une autre dans U également : c'est symétrique en T et U). Ces duades sont donc exactement les duades des 3 synthèmes de X correspondant aux 3 duades de A dans T. Ces 3 synthèmes sont 2 à 2 disjointes (elles appartiennent 2 à 2 au repère de X associé au point commun entre les duades de A correspondantes), mais ne font pas toutes les 3 parties d'un même repère de X (car les 3 duades de T n'ont pas de point en commun). Ces 3 synthèmes de X sont donc dans la configuration

(b) de la figure 9. En considérant les duades manquantes, on en déduit une $3+3$ partition de X :

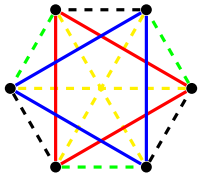


FIGURE 12. De 3 synthèmes incompatibles (jaune, vert et noir) on déduit une $3+3$ partition (bleu et rouge)

Cette construction est symétrique au sens suivant : étant donné une $3+3$ partition de $X = \tilde{U} \sqcup \tilde{V}$, on effectue la construction précédente pour obtenir une $3+3$ partition des repères de X qui sont les points de A via un des isomorphismes précédents. Si $X = \tilde{U} \sqcup \tilde{V}$ est obtenue à partir de $A = U \sqcup V$, la $3+3$ partition de A obtenue à partir de $\tilde{U} \sqcup \tilde{V}$ est à nouveau $U \sqcup V$.

En effet, on constate que les synthèmes de X que l'on considère pour former la $3+3$ partition de X à partir de $U \sqcup V$ sont exactement les synthèmes dont toutes les duades possèdent un élément de $\tilde{U}$ et un de $\tilde{V}$: ce sont les synthèmes complémentaires à celles qui contiennent une duade dans $\tilde{U}$ et une dans $\tilde{V}$ (qui nous ont permis d'associer U et V à $\tilde{U}$ et $\tilde{V}$). Donc U et V sont bien associés dans les deux sens.

8.3. L'automorphisme extérieur

- Les permutations de A induisent naturellement des permutations sur X, on note $\varphi : \mathfrak{S}_A \longrightarrow \mathfrak{S}_X$ le morphisme associé.
- Ce morphisme est un isomorphisme : Ceci découle de la dualité vue précédemment. En effet, si $\sigma \in \mathfrak{S}_X$ fixe X, elle fixe les repères de X donc A (plus précisément, σ fixe les intersections de X qui sont les synthèmes de A, puis les intersections de synthèmes qui sont les duades de A, puis les intersections de duades qui sont les points de A).
- Ce morphisme induit (via une numérotation de A et X) un automorphisme extérieur de $\mathfrak{S}_6$: on peut le voir de différentes manières :
  - L'image du stabilisateur d'un point agit transitivement sur les repères de A : il suffit d'envoyer deux synthèmes d'un repère (de A) sur deux autre synthèmes d'un autre repère ce qui est possible en fixant un point car deux synthèmes compatibles forment un cycle.
  - L'image d'une transposition est une triple transposition (aucun repère d'est stabilisé par une transposition $\tau = (a\ b)$ car les synthèmes 5 d'un repère dont $\{a, b\}$ n'est pas une duade sont envoyées sur une synthème incompatible, et la triple transposition est donnée par le synthème de X associé à la duade $\{a, b\}$).
  - L'image d'un 3-cycle est un double 3-cycle (donnée par la $3+3$ partition associée, reste juste à trouver le sens de deux cycles).

9. Construction d'un système de Steiner $S(5,6,12)$

On appellera hexades les parties de 6 éléments qui constitue un système de Steiner $S(5,6,12)$.

On considère l'ensemble $A \sqcup X$ dont les hexades sont les éléments suivants :

(a) A et X.

(b) 2 duades de A, et la duade de X associée à la synthème engendré par ces duades.

(b') La même chose que (b) mais en inversant A et X par dualité.

(c) 3 éléments de A et 3 éléments de X dans la $3+3$ partition associé (et donc la même chose dans l'autre sens aussi par symétrie de la construction de $3+3$ partition).

Vérifions que cet ensemble d'hexades forme bien un système de Steiner $S(5,6,12)$. On se donne donc $B \subset A \sqcup X$ un ensemble à 5 éléments. Par symétrie on peut supposer que $B \cap A > B \cap X$. Alors :

- Si $B \subset A$, A (de type (a)) convient.
- Si $|B \cap A| = 4$, $A \setminus B$ est une duade de A et engendre une synthème de X, une des duades D de cette synthème contient alors le point de $B \cap X$. Alors $(B \cap A) \sqcup D$ convient (de type (b)).
- Si $|B \cap A| = 3$, on considère la $3+3$ partition de X associée à celle de A dont les parties sont $A \cap B$ et $A \setminus B$. Alors
  - Si $B \cap X$ est incluse dans une des parties de cette partitions, une hexade de type (c) convient.
  - Sinon, par définition de la $3+3$ partition de X associée à celle de A, la duade $B \cap X$ correspond à une synthème de A possédant une duade dans $A \cap B$. Ainsi $A \cap B$ est recouvert par deux duades de cette synthème : on a une hexade de type (b) qui convient.

L'unicité de l'hexade contenant B vient du fait qu'il y a exactement $\frac{\binom{12}{5}}{\binom{6}{5}} = 132$, et nous en avons trouvé :

* 2 de type (a)
* $2 \times (15) = 90$ de type (b)
* $2 \times \binom{6}{3} = 40$ de type (c)

10. Unicité du système de Steiner $S(5,6,12)$

Soit S un système de Steiner $S(5,6,12)$.

Si H est une hexade, et $I \subset H$ une partie à i éléments, on remarque que le nombre d'hexades intersectant H en I ne dépend pas de H ou I et vaut :

$$M_{ii} = \begin{cases} \frac{\binom{12-i}{5-i}}{\binom{6-i}{5-i}} \text{ si } i \leqslant 5 \\ \\ 1 \text{ si } i = 6 \end{cases}$$

Soit $I \subset J \subset H$ où H est une hexade, avec $|I| = i$ et $|J| = j$. On définit M_{ij} ($i \leqslant j$) comme étant le nombre d'hexades K telles que $K \cap J = I$. On a vu que les $M_{i,6}$ ($i > 0$) ne dépendent pas des choix de I, J, H. On remarque que $M_{ij} = M_{i,j+1} + M_{i+1,j+1}$ (pour

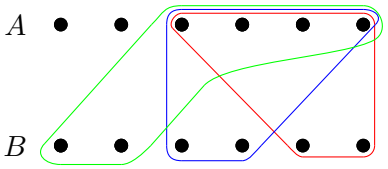
$x \in H \setminus J$ on partitionne les hexades selon si elles contiennent x ou non), et on en déduit par récurrence que M_{ij} ne dépend pas de I, J, H (mais H doit être une hexade). On obtient le tableau des M_{ij} suivant :

$$
\begin{array}{ccccccccccc}
 & & & & & 132 & & & & & \\
 & & & & 66 & & 66 & & & & \\
 & & & 30 & & 36 & & 30 & & & \\
 & & 12 & & 18 & & 18 & & 12 & & \\
 & 4 & & 8 & & 10 & & 8 & & 4 & \\
1 & & 3 & & 5 & & 5 & & 3 & & 1 \\
1 & & 0 & & 3 & & 2 & & 3 & & 0 & & 1
\end{array}
$$

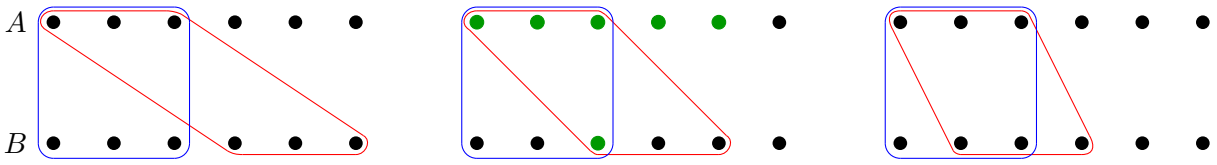
FIGURE 13. Triangle d'intersection

- $\underline{M_{0,6} = 1}$: Le complémentaire d'une duade est donc une duade. On peut donc fixer A et B deux hexades complémentaires.
- $\underline{M_{4,6} = 3}$: Cela nous permet d'associer une synthème de B à une duade de A (nous montrerons plus tard que cette association est injective et donc une correspondance).

  Soit D une duade de A, il existe 3 duades intersectant A en $A \setminus D$. Étant donné que deux hexades différentes ne peuvent pas s'intersecter en 5 points, leurs intersections avec B forment donc une synthème de B :



- $\underline{M_{3,6} = 2}$: Cela nous permet d'établir une correspondance entre les $3+3$ partitions de A et de B. Considérons les 2 hexades K et L intersectant A en exactement 3 points fixés. Il y a a priori 3 cas :



Montrons que seul le premier cas est possible, ce qui nous donnera la correspondance parfaitement symétrique entre les $3+3$ partitions de A et de B (car le complémentaire d'une hexade est une hexade).

— Le dernier cas est impossible que K et L s'intersectent en 5 points.

— Le deuxième cas est également impossible car si on considère le synthème associé à $K \setminus L \subset K$, une des duades est inclue dans A et l'hexade associée (points verts) intersecte donc A en 5 points.

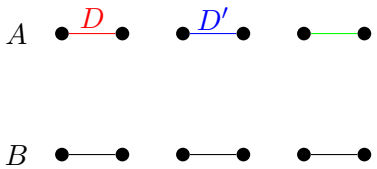
Cette construction est bijective car le rôle de A et B est parfaitement symétrique.

Montrons l'injectivité que nous avons mentionné pour $M_{4,6}$, c'est à dire montrons que 2 duades de A correspondent à 2 synthèmes de B différentes.

On suppose par l'absurde que $D \neq D'$ correspondent à la même synthème $T = \{t_1, t_2, t_3\}$.

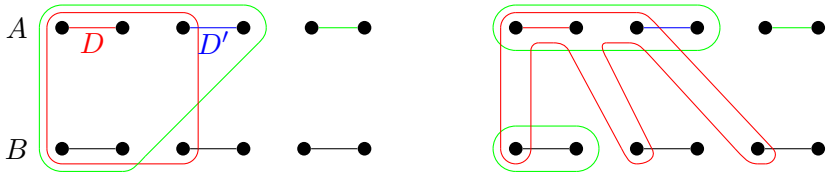
— D et D' sont disjointes car sinon $D \sqcup t_1 \sqcup t_2$ et $D' \sqcup t_1 \sqcup t_2$ sont deux hexades différentes partageant 5 points.

Nous sommes donc dans la configuration suivante :



où 3 duades de A et/ou B forment toujours une hexade (la dernière duade de A donne la même synthème par complémentarité des hexades).

Regardons les $3+3$ partitions de A et B pour trouver l'absurdité : il y a deux configurations possibles pour une $3+3$ partition contenant D :



— La première est absurde car les hexades rouges et vertes s'intersectent en 5 points.

— On est donc dans le deuxième cas. Cependant on peut trouver $3 \times 2 = 6$ partitions de A contenant une duade de la synthème $\{D, D', A \setminus (D \sqcup D')\}$ mais seulement $2 \times 2 = 10 - 6 = 4$ $3+3$ partitions de B ne contenant aucune des duades de la synthème de B. Ceci est absurde par la correspondance bijective entre les $3+3$ partitions de A et de B (vue en $M_{3,6}$).

Nous pouvons enfin conclure !

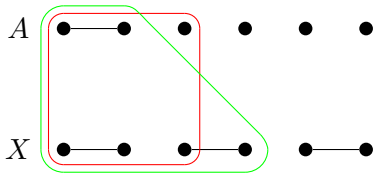
On considère l'ensemble X construit comme dans la partie 8 à partir de l'hexade A, et la bijection :

$$B \longrightarrow X$$
$$b \longmapsto \{\text{Synthèmes de } A \text{ associées à toutes les duades de } B \text{ contenant } b\}$$

qui nous permet de voir B comme X.

Il suffit à présent de constater que (via la bijection) S contient les hexades de type (a), (b) et (c) du système de Steiner de la partie 9 :

- Type (a) et (b) par définition (on peut passer au complémentaire pour voir qu'il y a les hexades intersectant A en 2 points).
- Type (c) : soit $A = U \sqcup T$ une $3+3$-partition. On remarque que la configuration suivante est impossible :



En considérant toutes les duades de T, on fixe donc totalement la $3+3$ partition de X tout comme on avait définit les $3+3$ partitions de X associées à A.

Nous avons ainsi montré l'unicité de $S(5,6,12)$ à conjugaison près ! Le groupe M_{12} est donc bien défini à isomorphisme près comme le stabilisateur de S.

Il découle de plus que M_{12} agit exactement 5-transitivement. En effet, si $(x_1,\dots,x_5)$ et $(y_1,\dots,y_5)$ sont deux 5-uplets de points distincts, il existe une (unique) hexade $\{x_1,\dots,x_6\}$ (resp. $\{y_1,\dots,y_6\}$) contenant $\{x_1,\dots,x_5\}$ (resp. $\{y_1,\dots,y_5\}$). La permutation envoyant x_i sur y_i et le complémentaire de $\{x_1,\dots,x_6\}$ sur celui de $\{y_1,\dots,y_6\}$ via la bijection entre B et X vue précédemment est une permutation envoyant $(x_1,\dots,x_5)$ sur $(y_1,\dots,y_5)$. De plus si une permutation fixe $(x_1,\dots,x_5)$, elle fixe $\{x_1,\dots,x_6\}$ puis tous les points (via la bijection).

Plus précisément, prenons $A=\{1,\dots,6\}$ et X l'ensemble des repères de A. On considère d'une part la bijection φ_1 envoyant x_i sur i et $S\setminus\{x_1,\dots,x_6\}$ sur X via la bijection construite précédemment. Elle envoie les hexades de S sur les hexades de $A\sqcup X$. On obtient de même φ_2 en envoyant y_i sur i et $S\setminus\{y_1,\dots,y_6\}$ sur X. Alors $\varphi_2^{-1}\circ\varphi_1$ envoie $(x_1,\dots,x_5)$ sur $(y_1,\dots,y_5)$ et stabilise les hexades de S.

Documentation et sources

[1] John H. Conway, Noam D. Elkies, Jeremy L. Martin. — *The Mathieu group M_{12} and the M_{13} game.* Experimental Mathematics 15, no. 2 (2006), 223-236.

[2] Peter J. Cameron. — *From M_{12} to M_{24}.*

[3] R. M. Wilson. — *Graph puzzles, homotopy, and the alternating group.* J. Combin. Theory (Série B) 16 (1974) 86-96.

Mai 2024

Elias Giraud-Audine, Quentin Palazon