Journées mathématiques X-UPS

Année 2000

Groupes finis

Michel BROUÉ

Sur quelques groupes simples sporadiques

Journées mathématiques X-UPS (2000), p. 57-80.
https://doi.org/10.5802/xups.2000-02

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
2000, p. 57–80 doi: 10.5802/xups.2000-02

SUR QUELQUES GROUPES SIMPLES SPORADIQUES

par

Michel Broué

Table des matières

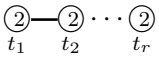
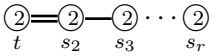
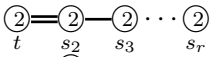
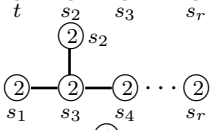
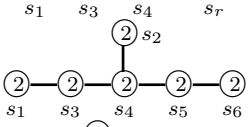
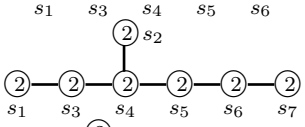
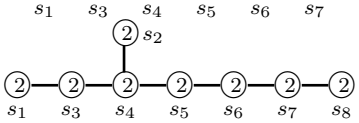
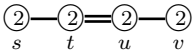
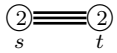
0. Introduction

Il semble que la liste des groupes finis simples (à isomorphisme près) soit connue. Elle se compose(rait) des séries suivantes :

- pour tout nombre premier p, le groupe cyclique $\mathsf{Z}/p\mathsf{Z}$,
- pour tout entier $n > 5$, le groupe alterné $\mathfrak{A}_n$,
- pour tout diagramme de Dynkin $\mathcal{D}_n$ et toute puissance q d'un nombre premier (hormis quelques petites valeurs de n et de q), un groupe $G(\mathcal{D}_n, q)$ donné par la table 1.
- pour toute version « tordue » d'un diagramme de Dynkin ${}^t\mathcal{D}_n$ et toute puissance q d'un nombre premier (hormis quelques petites

Publication originelle dans Journées X-UPS 2000. Groupes finis. Éditions de l'École polytechnique, 2000.

Table 1.

Type A_r :		$- - - - \to$	$\mathsf{PSL}_{r+1}(q)$
Type B_r :		$- - - - \to$	$\mathsf{PSO}_{2r+1}(q)$
Type C_r :		$- - - - \to$	$\mathsf{PSp}_{2r}(q)$
Type D_r :		$- - - - \to$	$\mathsf{PSO}_{2r}(q)$
Type E_6 :		$- - - - \to$	$\mathsf{E}_6(q)$
Type E_7 :		$- - - - \to$	$\mathsf{E}_7(q)$
Type E_8 :		$- - - - \to$	$\mathsf{E}_8(q)$
Type F_4 :		$- - - - \to$	$\mathsf{F}_4(q)$
Type G_2 :		$- - - - \to$	$\mathsf{G}_2(q)$

valeurs de n et de q), un groupe $G({}^t\mathcal{D}_n, q)$:

Type ${}^2\mathsf{A}_r$:	$- - - - \to$	$\mathsf{PSU}_{r+1}(q)$
Type ${}^2\mathsf{D}_r$:	$- - - - \to$	$\mathsf{PSO}^-_{2r}(q)$
Type ${}^3\mathsf{D}_4$:	$- - - - \to$	${}^3\mathsf{D}_4(q)$,

et pour toute version « très tordue » (combinant un automorphisme de l'espace vectoriel réel des racines avec un automorphisme de corps), un groupe ${}^tG(\mathcal{D}_n, q)$:

Type B_2 :	$q = 2^{2n+1}$	$- - - - \to$	${}^2\mathsf{B}_2(q)$
Type F_4 :	$q = 2^{2n+1}$	$- - - - \to$	${}^2\mathsf{F}_4(q)$
Type G_2 :	$q = 3^{2n+1}$	$- - - - \to$	${}^2\mathsf{G}_2(q)$

- 26 autres groupes, appelés les « groupes simples sporadiques ».

- Le plus grand d'entre eux, appelé « le Monstre », est d'ordre

$$2^{46}3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71.$$

- Les plus anciennement connus d'entre eux sont les cinq « groupes de Mathieu » M_{11}, M_{12}, M_{22}, M_{23}, M_{24} (cf. [Mat73]).

1. Un peu d'algèbre linéaire et multilinéaire sur F_2

Notation. Si n est un entier naturel, on note $n=\sum_{k>0} b_k(n)2^k$ son développement binaire (ainsi, $b_k(n)\in\{0,1\}$). On vérifie alors que $b_k(n)\equiv\binom{n}{2^k} \mod 2$. On considère dorénavant b_k comme une application de N sur $\mathsf{Z}/2\mathsf{Z}$.

Si E est un ensemble, on note $|E|$ son cardinal.

L'espace $\mathcal{P}(\Omega)$ et les formes invariantes par $\mathfrak{S}(\Omega)$. Soit Ω un ensemble fini de cardinal n. L'ensemble des parties de Ω, muni de l'opération *di érence symétrique* (définie par $x+y:=(x\cup y)-(x\cap y)$) est un espace vectoriel sur F_2, naturellement isomorphe à F_2^{Ω}. On le note $\mathcal{P}(\Omega)$.

On peut vérifier les propriétés suivantes.

(1) Il existe une et une seule forme linéaire non triviale sur $\mathcal{P}(\Omega)$ invariante par l'action du groupe symétrique $\mathfrak{S}(\Omega)$, à savoir la forme

$$\tau\,\mathcal{P}(\Omega)\longrightarrow \mathsf{F}_2,\quad x\longmapsto b_0(|x|).$$

Le noyau de τ est l'hyperplan $\mathcal{H}(\Omega)$, ensemble des parties de cardinal pair de Ω.

(2) L'ensemble des formes bilinéaires symétriques sur $\mathcal{P}(\Omega)$ invariantes par $\mathfrak{S}(\Omega)$ est un espace vectoriel de dimension 2 sur F_2. Il est constitué de la forme nulle et des trois formes suivantes :

- $(x,y)\mapsto\tau(x\cap y)$,
- $(x,y)\mapsto\tau(x)\tau(y)$,
- $(x,y)\mapsto\tau(x\cap y)+\tau(x)\tau(y)$.

On pose $\langle x,y\rangle:=\tau(x\cap y)$. La forme $\langle -,-\rangle$ est non dégénérée. Pour $x\subseteq\Omega$, on note x^0 l'orthogonal de x pour cette forme. Soit $\mathcal{D}(\Omega):=\mathcal{H}(\Omega)^0$. On a $\mathcal{D}(\Omega)=\{\,?\,,\Omega\}$, et si n est pair on a $\mathcal{D}(\Omega)\subseteq\mathcal{H}(\Omega)$.

(3) Une forme quadratique sur $\mathcal{P}(\Omega)$ invariante par $\mathfrak{S}(\Omega)$ est une application $\varphi\,\mathcal{P}(\Omega) \to \mathsf{F}_2$ telle que l'application $(x,y) \mapsto \varphi(x+y) - \varphi(x) - \varphi(y)$ est une forme bilinéaire sur $\mathcal{P}(\Omega)$ invariante par $\mathfrak{S}(\Omega)$.

L'ensemble des formes quadratiques sur $\mathcal{P}(\Omega)$ invariantes par $\mathfrak{S}(\Omega)$ est un espace vectoriel de dimension 2 sur F_2. Il est constitué de la forme nulle et des trois formes quadratiques suivantes :

- $x \mapsto \varphi(x) := b_1(|x|)$,
- $x \mapsto \tau(x)$,
- $x \mapsto \psi(x) := \tau(x) + q(x)$.

On a $\varphi(x+y)-\varphi(x)-\varphi(y) = \psi(x+y)-\psi(x)-\psi(y) = \langle x,y\rangle+\tau(x)\tau(y)$. Les formes φ et ψ ont même restriction, notée q, à l'hyperplan $\mathcal{H}(\Omega)$, telle que

$$q(x) = \frac{|x|}{2} \mod 2 \quad \text{pour tout } x \in \mathcal{H}(\Omega),$$

et

$$q(x+y) - q(x) - q(y) = \langle x,y\rangle \quad \text{pour tous } x,y \in \mathcal{H}(\Omega).$$

Classification. Lluis Puig a classifié les espaces quadratiques

$$(\mathcal{P}(\Omega),\varphi), \quad (\mathcal{P}(\Omega),\psi) \quad \text{et} \quad (\mathcal{H}(\Omega),q).$$

Pour énoncer son résultat, on introduit les notations suivantes.

- Pour tout entier pair $n = 2k$, on note H_n l'espace F_2^n muni de la forme quadratique définie ainsi : si $(e_i)_{1 \leqslant i \leqslant n}$ est la base canonique de F_2^n, les espaces engendrés par $(e_i)_{1 \leqslant i \leqslant k}$ et $(e_i)_{k+1 \leqslant i \leqslant n}$ sont totalement singuliers et pour tout $i \leqslant k$, le produit scalaire de e_i avec e_{k+j} est $\delta_{i,j}$.
- On note N_1 l'espace de dimension 1 sur F_2 muni de la forme quadratique nulle.
- On note I_1 l'espace de dimension 1 sur F_2 muni de la forme quadratique non nulle.
- On note I_2 l'espace de dimension 2 sur F_2 muni de la forme quadratique définie par $(\lambda,\mu) \mapsto \lambda + \mu + \lambda\mu$.

1.1. Théorème. *Les types d'isomorphismes des espaces quadratiques $(\mathcal{P}(\Omega),\varphi)$, $(\mathcal{P}(\Omega),\psi)$ et $(\mathcal{H}(\Omega),q)$ ne dépendent que de la valeur de $n \mod 8$, et sont donnés par le tableau* 2.

Table 2.

$n \bmod 8$	$(\mathcal{P}(\Omega), \varphi)$	$(\mathcal{P}(\Omega), \psi)$	$(\mathcal{H}(\Omega), q)$
0	H_n	H_n	$N_1 \perp H_{n-2}$
1	$N_1 \perp H_{n-1}$	$I_1 \perp H_{n-1}$	H_{n-1}
2	H_n	$I_2 \perp H_{n-2}$	$I_1 \perp H_{n-2}$
3	$I_1 \perp H_{n-1}$	$N_1 \perp I_2 \perp H_{n-3}$	$I_2 \perp H_{n-3}$
4	$I_2 \perp H_{n-2}$	$I_2 \perp H_{n-2}$	$N_1 \perp I_2 \perp H_{n-4}$
5	$N_1 \perp I_2 \perp H_{n-3}$	$I_1 \perp H_{n-1}$	$I_2 \perp H_{n-3}$
6	$I_2 \perp H_{n-2}$	H_n	$I_1 \perp H_{n-2}$
7	$I_1 \perp H_{n-1}$	$N_1 \perp H_{n-1}$	H_{n-1}

Codes autoduaux pairs. Introduisons quelques définitions.

- Un *code correcteur d'erreurs* (ou simplement « code ») est un sous-espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.
- Un code $\mathcal{E}$ est dit *entier* s'il est contenu dans son orthogonal $\mathcal{E}^0$. Un code $\mathcal{E}$ est dit *auto-orthogonal* s'il est égal son orthogonal $\mathcal{E}^0$.

Ainsi, un code $\mathcal{E}$ est entier si et seulement si, pour tous $x, y \in \mathcal{E}$, $|x \cap y|$ est pair. En particulier, on a $\mathcal{E} \subseteq \mathcal{H}(\Omega)$.

- Un code $\mathcal{E}$ est dit *pair* si, pour tout $x \in \mathcal{E}$, $|x|$ est divisible par 4.

Un code pair est contenu dans $\mathcal{H}(\Omega)$ et totalement singulier pour la forme quadratique q, donc il est entier.

Le résultat suivant est alors facile à déduire du théorème 1.1.

1.2. Théorème. *Il existe un code auto-orthogonal et pair dans $\mathcal{P}(\Omega)$ si et seulement si $n \equiv 0 \mod 8$.*

Exercice. Supposons $n = 2m$, et posons

$$\Omega := \{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m\}.$$

Alors le code engendré par tous les éléments de la forme

$$x_{i,j} := \{\alpha_i, \alpha_j, \beta_i, \beta_j\}$$

où $1 \leq i, j \leq m$ et $i \neq j$, et par $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, est de dimension m. Il est entier, donc auto-orthogonal si m est pair. Il est pair (et auto-orthogonal) si m est multiple de 4.

Le paragraphe suivant nous fournira des exemples intéressants de codes autoduaux pairs.

Polynôme des poids d'un code. Le *polynôme des poids* d'un code $\mathcal{E}$ est par définition

$$P_{\mathcal{E}}(X, Y) := \sum_{x \in \mathcal{E}} X^{|x|} Y^{n-|x|}.$$

Le résultat suivant, qui permet de calculer le polynôme des poids du code orthogonal $\mathcal{E}^0$ en fonction du polynôme des poids de $\mathcal{E}$, est connu sous le nom de *formule de MacWilliams*.

1.3. Théorème. *Pour tout code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on a*

$$P_{\mathcal{E}^0}(X, Y) = 2^{(n/2)-\dim \mathcal{E}} \frac{1}{\sqrt{2}} P_{\mathcal{E}}(-X + Y, X + Y).$$

Si $P(X, Y) \in \mathbb{C}[X, Y]$ et si $g := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est une matrice à coefficients complexes, on note $P \cdot g$ le polynôme défini par

$$(P \cdot g)(X, Y) := P(aX + bY, cX + dY).$$

1.4. Corollaire. *Si $\mathcal{E}$ est un code auto-orthogonal pair, alors son polynôme des poids est invariant par l'action (à droite) du sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices*

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{et} \quad \tau := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

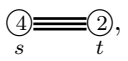
Or les deux matrices ρ et τ représentent des *pseudo-réflexions* (i.e., des automorphismes d'ordre fini dont l'espace des points fixes est un hyperplan), et le groupe W qu'elles engendrent est un groupe *fini* : c'est un *groupe de réflections complexes* d'ordre 192, noté G_9 dans la classification de Shephard et Todd.

```
gap> r2 := (E(8) + E(8)^7)/2;
  1/2*E(8)-1/2*E(8)^3
gap> rho := [[E(4),0],[0,1]];
  [ [ E(4), 0 ], [ 0, 1 ] ]
```

```
gap> tau := r2*[[-1,1],[1,1]];
  [ [ -1/2*E(8)+1/2*E(8)^3, 1/2*E(8)-1/2*E(8)^3 ],
    [ 1/2*E(8)-1/2*E(8)^3, 1/2*E(8)-1/2*E(8)^3 ] ]
gap> Size(Group(rho,tau));
  192
```

———

Exercice. Le groupe W est représenté par le diagramme



i.e., est défini par deux générateurs s et t satisfaisant les relations

$$s^4 = t^2 = 1 \quad \text{et} \quad ststst = tststs.$$

Les *degrés* du groupe W (cf. [Bou68], § 5) sont 8 et 24, i.e., l'algèbre $\mathbb{C}[X,Y]^W$ des polynômes invariants par l'action de W est engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24. On en déduit :

1.5. Proposition. *La dimension de l'espace vectoriel des polynômes homogènes de degré n invariants par W est $1 + [n/24]$.*

Plus précisément, on peut démontrer que l'algèbre $\mathbb{Z}[X,Y]^W$ de polynômes à coefficients *entiers* et invariants par W est engendrée par les deux polynômes

$$\begin{cases} A(X,Y) := \dfrac{1}{2}\left[(X^2+Y^2)^4 + (X^2-Y^2)^4 + (2XY)^4\right], \\ D(X,Y) := X^4Y^4(X^4-Y^4)^4. \end{cases}$$

1.6. Corollaire

(1) *Il y a un seul polynôme qui peut être le polynôme des poids d'un code auto-orthogonal et pair en dimension 8, à savoir le polynôme*

$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8.$$

(2) *Il y a un seul polynôme qui peut être le polynôme des poids d'un code auto-orthogonal et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme*

$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}.$$

Nous allons voir au paragraphe suivant qu'il existe effectivement un code auto-orthogonal pair en dimension 24 ne contenant aucun vecteur de poids 4. Ce code a pour groupe d'automorphismes le groupe de Mathieu M_{24}.

2. Systèmes de Steiner et groupes de Mathieu

Définition. Soient x, c, n trois entiers tels que $1 \leq x \leq c \leq n$. Un système de Steiner de type $\mathrm{St}(x, c, n)$ est la donnée

- d'un ensemble Ω de cardinal n,
- d'un ensemble $\mathcal{C}$ de parties de Ω, toutes de cardinal c, appelées les cellules,

telle que, pour tout sous-ensemble X de cardinal x de Ω, il existe une et une seule cellule contenant X.
Le groupe des automorphismes d'un système de Steiner $(\Omega, \mathcal{C})$ est le sous-groupe du groupe symétrique $\mathfrak{S}_\Omega$ de Ω formé des permutations qui stabilisent (globalement) $\mathcal{C}$.

Exemples faciles

(a) La famille Ω_c de toutes les parties de Ω de cardinal c définit un système de Steiner $\mathrm{St}(c, c, n)$.

(b) Si q est une puissance d'un nombre premier, les droites de l'espace affine de dimension n sur F_q définissent un système de Steiner $\mathrm{St}(2, q, q^n)$.

La proposition suivante fournit des conditions arithmétiques sur les entiers (x, c, n) nécessaires pour l'existence d'un système de Steiner de type $\mathrm{St}(x, c, n)$: on les obtient en écrivant que les quotients de coefficients du binômes considérés sont des entiers.

2.1. Proposition. *Supposons qu'il existe un système de Steiner $(\Omega, \mathcal{C})$ de type $\mathrm{St}(x, c, n)$.*

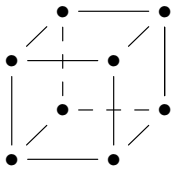
(1) *On a*

$$|\mathcal{C}| = \binom{n}{x} \Big/ \binom{c}{x}.$$

(2) *Plus généralement, pour tout entier $y \leq x$, le nombre $|\mathcal{C}_Y|$ d'éléments de $\mathcal{C}$ qui contiennent un sous-ensemble donné Y de cardinal y est*

$$|\mathcal{C}_Y| = \binom{n-y}{x-y} \Big/ \binom{c-y}{x-y}.$$

Le système de Steiner de type $\mathrm{St}(3,4,8)$**.** Les plans de l'espace a□ne de dimension 3 sur le corps F_2 peuvent être vus comme tous les sous-ensembles des sommets d'un cube formés de l'union des sommets de deux côtés parallèles.



Il y 14 tels plans. Il est clair qu'ils forment un système de Steiner de type $\mathrm{St}(3,4,8)$.

Désignons par Ω l'ensemble sous-jacent à F_2^3. On voit que les cellules de ce système de Steiner engendrent un code auto-orthogonal pair dans $\mathcal{P}(\Omega)$.

Réciproquement, si $\mathcal{E}$ est un code auto-orthogonal pair dans $\mathcal{P}(\Omega)$ où Ω est un ensemble de cardinal 8, l'ensemble $\mathcal{C}$ des éléments de poids 4 de $\mathcal{E}$ forme un système de Steiner de type $\mathrm{St}(3,4,8)$.

[En e□et, par trois points de Ω passe au plus un élément de $\mathcal{C}$ (la somme de deux éléments de cardinal 4 ayant trois points en commun est de cardinal 2). Or on sait (cf. 1.6, (1)) que $|\mathcal{C}| = 14$. Comme $14 = \binom{8}{3}/\binom{4}{3}$, on voit qu'en fait il passe un élément de $\mathcal{C}$ par tout triplet.]

Les propriétés suivantes sont laissées à titre d'exercice.

- Un système de Steiner de type $\mathrm{St}(3,4,8)$ est unique à isomorphisme près : si $(\Omega,\mathcal{C})$ et $(\Omega',\mathcal{C}')$ sont deux systèmes de Steiner de type $\mathrm{St}(3,4,8)$, il existe une bijection de Ω sur Ω' qui induit une bijection de $\mathcal{C}$ sur $\mathcal{C}'$.
- Si $(\Omega,\mathcal{C})$ est un système de Steiner de type $\mathrm{St}(3,4,8)$, son groupe d'automorphismes est isomorphe au groupe a□ne de dimension 3 sur le corps à deux éléments, i.e., isomorphe à $(\mathsf{Z}/2\mathsf{Z})^3 \circ \mathrm{GL}_3(\mathsf{F}_2)$, groupe d'ordre $2^6 \cdot 3 \cdot 7$.

Une construction du groupe de Mathieu M_{12}**.** Considérons les deux battages de 12 cartes suivant :

- On tient le paquet dans la main gauche, faces dessus. On passe la première carte du paquet dans la main droite, toujours face vers le

haut. On pose la deuxième carte du paquet sur la carte de droite, puis la troisième sous le paquet de droite, la quatrième dessus, la cinquième dessous, etc. Quand toutes les cartes sont passées de gauche à droite, on reprend le paquet dans la main gauche.

Le passage du paquet originel au paquet final définit la permutation suivante

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 10 & 8 & 6 & 4 & 2 & 1 & 3 & 5 & 7 & 9 & 11 \end{pmatrix},$$

i.e., le produit de cycles

$$(1,\, 12,\, 11,\, 9,\, 5,\, 4,\, 6,\, 2,\, 10,\, 7)(3,\, 8),$$

une permutation d'ordre 10.

• On tient le paquet dans la main gauche, faces dessus. On passe la première carte du paquet dans la main droite, toujours face vers le haut. On pose la deuxième carte du paquet sous la carte de droite, puis la troisième sur le paquet de droite, la quatrième dessous, la cinquième dessus, etc. Quand toutes les cartes sont passées de gauche à droite, on reprend le paquet dans la main gauche.

Le passage du paquet originel au paquet final définit la permutation suivante

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 9 & 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 & 10 & 12 \end{pmatrix},$$

i.e., le cycle

$$(1,\, 11,\, 10,\, 8,\, 4,\, 5,\, 3,\, 7,\, 2,\, 9,\, 6),$$

une permutation d'ordre 11.

Les deux permutations précédentes engendrent le groupe de Mathieu M_{12}, qui est 5 fois transitif sur 12 lettres :

———

```
gap> M := Group([(1,12,11,9,5,4,6,2,10,7)(3,8),(1,11,10,8,4,5,3,7,2,9,6)],()) ;
     Group( ( 1,12,11, 9, 5, 4, 6, 2,10, 7)( 3, 8), ( 1,11,10, 8, 4, 5,
3, 7, 2, 9, 6) )
gap> Size(M) ;
     95040
gap> 12*11*10*9*8 ;
     95040
```

On aurait aussi pu demander

```
gap> NrArrangements([1..12],5) ;
```

```
95040 gap> Length(Orbits(M,[[1,2,3,4,5]],OnTuples));
1
```

Le calcul du nombre d'orbites a été e ectué en trois heures sur un Mac G4 – 450 MHz avec le logiciel (gratuit) GAP. Il est beaucoup plus économique de demander

```
gap>
Size(Intersection(Stabilizer(M,1),Stabilizer(M,2),Stabilizer(M,3),
   Stabilizer(M,4), Stabilizer(M,5)));
```

ou plus simplement

```
gap> Size(Stabilizer(M,[1..5],OnTuples));
1
```

On peut démontrer que le groupe de Mathieu M_{12} est le groupe des automorphismes d'un système de Steiner de type $\mathrm{St}(5,6,12)$.

Le groupe de Mathieu M_{11} est par définition le stabilisateur d'un point dans M_{12}.

Le stabilisateur de deux points (stabilisateur d'un point dans la représentation 4 fois transitive de M_{11} sur 11 points), noté M_{10}, opère naturellement sur 10 points. Il est de même ordre que le groupe projectif $\mathrm{PGL}_2(\mathsf{F}_9)$ (qui opère naturellement sur la droite projective $\mathsf{P}^1(\mathsf{F}_9)$)... mais ne lui est pas isomorphe. Cependant, les groupes dérivés M'_{10} et $\mathrm{PSL}_2(9)$ sont isomorphes, et isomorphes à $\mathfrak{A}_6$: les groupes $\mathfrak{S}_6$, M_{10} et $\mathrm{PGL}_2(\mathsf{F}_9)$ sont les trois sous-groupes d'indice 2 du groupe $\mathrm{Aut}(\mathfrak{A}_6)$ des automorphismes de $\mathfrak{A}_6$. Ils sont mutuellement non isomorphes.

Le groupe de Mathieu M_{24} ***et le système de Steiner de type*** $\mathrm{St}(5,8,24)$

1. Le groupe de Mathieu M_{24} est un groupe 5 fois transitif sur 24 lettres (cf. [Mat73], d'ordre

$$|\mathrm{M}_{24}| = 2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23 = 48\cdot(24\cdot 23\cdot 22\cdot 21\cdot 20).$$

On peut le construire de la manière suivante.

Soit $\Omega := \mathsf{P}^1(\mathsf{F}_{23}) = \mathsf{F}_{23}\cup\{\infty\}$.

• Soit c un générateur du groupe des carrés de $\mathsf{F}_{23}^\times$. Alors les trois permutations suivantes de Ω

$$\alpha\longmapsto\alpha+1,\quad \alpha\longmapsto c\alpha,\quad \alpha\longmapsto -\alpha^{-1}$$

engendrent le groupe $\mathrm{PSL}_2(23)$ dans son opération sur la droite projective.

- On leur adjoint la permutation de Ω définie par

$$\alpha \longmapsto \begin{cases} \alpha^3/9 & \text{si } \alpha \text{ est un carré dans } \mathsf{F}_{23}^\times, \\ 9\alpha^3 & \text{sinon.} \end{cases}$$

On définit alors M_{24} comme le sous-groupe de $\mathfrak{S}(\Omega)$ engendré par les quatre permutations ci-dessus.

Exercice. Utiliser GAP pour calculer l'ordre du groupe engendré par les quatre permutations précédentes.

2. On construit un code $\mathcal{E}$ auto-orthogonal et pair dans $\mathcal{P}(\Omega)$ invariant par le groupe M_{24} de la façon suivante.

Soit N l'ensemble des 11 non-carrés de F_{23}. Pour tout $\alpha \in \mathsf{F}_{23}$, on pose

$$N_\alpha := \{\beta - \alpha \mid (\beta \in N)\}.$$

On définit 23 sous-ensembles de cardinal 12 de Ω en posant :

$$D_\alpha := \{\infty\} \cup N_\alpha.$$

Enfin, on note $\mathcal{E}$ le sous-espace de $\mathcal{P}(\Omega)$ engendré par le système

$$\{\Omega\} \cup \{D_\alpha \mid (\alpha \in \mathsf{F}_{23})\}.$$

Posant $D_\infty := \Omega$, et pour tout $x \subseteq \Omega$, on note $D_x := \sum_{\alpha \in x} D_\alpha$.

2.2. Théorème

(1) *L'application linéaire $\mathcal{P}(\Omega) \to \mathcal{E}$, $x \mapsto D_x$ a pour noyau $\mathcal{E}$ et définit un isomorphisme $\mathcal{P}(\Omega)/\mathcal{E} \xrightarrow{\sim} \mathcal{E}$.*

(2) *L'espace $\mathcal{E}$ est un code auto-orthogonal pair stable par M_{24}.*

(3) *Il n'y a pas de vecteur de poids 4 dans $\mathcal{E}$, et les vecteurs de poids 8 sont les cellules d'un système de Steiner $\mathrm{St}(5, 8, 24)$.*

Indications succinctes sur la démonstration. On laisse au lecteur la tâche de démontrer les deux premières assertions. Démontrons la troisième.

Comme M_{24} est 5 fois transitif, si $\mathcal{E}$ contenait un vecteur de poids 4 il contiendrait tous les vecteurs de poids 4, donc ceux de poids 2, et il ne pourrait pas être auto-orthogonal.

On sait alors (cf. 1.6) que le polynôme des poids de $\mathcal{E}$ est

$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}.$$

Ainsi il y a 759 vecteurs de poids 8 dans $\mathcal{E}$. Deux tels vecteurs distincts ne peuvent s'intersecter en plus de 4 points (sinon leur somme serait de poids strictement inférieur à 6). Donc par 5 points il passe exactement un vecteur de poids 8 de $\mathcal{E}$.

De plus, on peut démontrer :

- Un système de Steiner de type $\mathrm{St}(5,8,24)$ est unique à isomorphisme près : si $(\Omega,\mathcal{C})$ et $(\Omega',\mathcal{C}')$ sont deux systèmes de Steiner de type $\mathrm{St}(5,8,24)$, il existe une bijection de Ω sur Ω' qui induit une bijection de $\mathcal{C}$ sur $\mathcal{C}'$.

- Si $(\Omega,\mathcal{C})$ est un système de Steiner de type $\mathrm{St}(5,8,24)$, son groupe d'automorphismes est isomorphe au groupe M_{24} et l'ensemble de ses cellules engendre un code auto-orthogonal pair.

Remarque. En remplaçant le nombre 23 par un autre nombre premier p congru à -1 modulo 8, on peut construire comme ci-dessus un code $\mathcal{E}$ auto-orthogonal et pair dans $\mathcal{P}(\mathrm{P}^1(\mathrm{F}_p))$. Mais si $p \neq 23$, le groupe des automorphismes de $\mathcal{E}$ est égal à $\mathrm{PSL}_2(p)$. Le cas où $p = 23$, cas où le groupe des automorphismes de $\mathcal{E}$ est strictement plus grand que $\mathrm{PSL}_2(p)$, est « exceptionnel ».

Appendice : le triangle de Conway d'un système de Steiner. Supposons qu'il existe un système de Steiner $(\Omega,\mathcal{C})$ de type $\mathrm{St}(x,c,n)$.

Soient z et y deux entiers tels que $z \leq y \leq c$. Soient Y et Z deux sous-ensembles d'une cellule, de cardinaux respectifs y et z, et tels que $Z \subseteq Y$. Alors le nombre de cellules dont l'intersection avec Y est égale à Z ne dépend que du couple (y,z) (et pas du choix de Y et Z). On note $\iota(y,z)$ ce nombre.

Pour tous y et z tels que $0 \leq z < y < c$, on a

$$\iota(y,z) = \iota(z+1,y) + \iota(z+1,y+1).$$

Cette formule permet de calculer par itération tous les nombres $\iota(y,z)$ à partir des nombres $\iota(y,y)$ qui, eux, sont donnés par la formule

$$\iota(y,y) = \begin{cases} \binom{n-y}{x-y} \Big/ \binom{c-y}{x-y} & \text{si } y \leq x, \\ 1 & \text{si } x \leq y \leq c. \end{cases}$$

• Pour un système de Steiner de type $\mathrm{St}(3,4,8)$, le tableau suivant fournit les valeurs de $\iota(y,z)$.

				$z{=}0$ ↙					
$y{=}0 \longrightarrow$				**14**	1 ↙				
$y{=}1 \longrightarrow$			7		**7**	2 ↙			
$y{=}2 \longrightarrow$		3		4		**3**	3 ↙		
$y{=}3 \longrightarrow$	1		2		2		**1**	4 ↙	
$y{=}4 \longrightarrow$	1	0		2		0		**1**	

• Pour un système de Steiner de type $\mathrm{St}(5,8,24)$, le tableau suivant fournit les valeurs de $\iota(y,z)$.

								$z{=}0$ ↙							
$y{=}0 \longrightarrow$								**759**	1 ↙						
$y{=}1 \longrightarrow$							506		**253**	2 ↙					
$y{=}2 \longrightarrow$						330		176		**77**	3 ↙				
$y{=}3 \longrightarrow$					210		120		56		**21**	4 ↙			
$y{=}4 \longrightarrow$				130		80		40		16		**5**	5 ↙		
$y{=}5 \longrightarrow$			78		52		28		12		4		**1**	6 ↙	
$y{=}6 \longrightarrow$		46		32		20		8		4		0		**1**	7 ↙
$y{=}7 \longrightarrow$	30		16		16		4		4		0		0		**1**
$y{=}8 \longrightarrow$	30	0		16		0		4		0		0		0	**1**

3. Réseaux unimodulaires pairs

Quelques définitions. On suppose $\mathbb{Q}^n$ muni de son produit scalaire naturel, noté $(x,y) \mapsto \langle x,y \rangle$. On note $x^2 := \langle x,x \rangle$.

Un réseau de $\mathbb{Q}^n$ est un sous-groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.

Soit L un réseau de $\mathbb{Q}^n$.

• Le dual L^0 de L est par définition l'ensemble des éléments $y \in \mathbb{Q}^n$ tels que $\langle x, y\rangle \in \mathbb{Z}$ pour tout $x \in L$.

Le groupe L^0 est un réseau dans $\mathbb{Q}^n$: si L a pour base $(v_1, v_2, \ldots, v_n)$, L^0 a pour base la base duale, i.e., la base $(v_1^0, v_2^0, \ldots, v_n^0)$ de $\mathbb{Q}^n$ définie par les conditions $\langle v_i, v_j^0\rangle = \delta_{i,j}$. L'application $L^0 \to \mathrm{Hom}(L, \mathbb{Z}), y \mapsto (x \mapsto \langle x, y\rangle)$ est un isomorphisme. On a $L^{00} = L$.

• Le volume $\mathrm{vol}(L)$ de L est la valeur absolue du déterminant d'une base de L par rapport à une base orthonormale de $\mathbb{Q}^n$. On a

$$\mathrm{vol}(L)\mathrm{vol}(L^0) = 1.$$

• Si l et L' sont des réseaux de $\mathbb{Q}^n$, il en est de même de $L \cap L'$ et $L + L'$. De plus on a $(L \cap L')^0 = L^0 + L'^0$ et $(L + L')^0 = L^0 \cap L'^0$.

Si $L \subseteq L'$ alors $L'^0 \subseteq L^0$, et $L'/L = \mathrm{Hom}(L^0/L'^0, \mathbb{Q}/\mathbb{Z})$, donc L'/L et L^0/L'^0 sont des groupes abéliens isomorphes, d'ordre $\mathrm{vol}(L)$.

• Le réseau L est dit *entier* si $L \subseteq L^0$, et *unimodulaire* si $L = L^0$. Il est dit *pair* si $x^2 \in 2\mathbb{Z}$ pour tout $x \in L$ (un réseau pair est entier).

• Si $r \in \mathbb{Q}$, le réseau L est dit *r-modulaire trivial* s'il admet une base $(v_1, v_2, \ldots, v_n)$ orthogonale et telle que $v_i^2 = 1/r$. On a alors $L^0 = rL$.

Le *groupe des automorphismes* d'un réseau L, noté $\mathrm{Aut}(L)$, est l'ensemble des isométries de $\mathbb{Q}^n$ dans lui-même qui envoient L sur lui-même.

Exemples

• Si $n = 2m$ (m entier), pour tout entier k, il existe un réseau 2^k-modulaire trivial.

En effet, soit $(e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{Q}^n$.

– Si $k = 2j$, le réseau de base $(2^{-j}e_1, 2^{-j}e_2, \ldots, 2^{-j}e_n)$ est 2^k-modulaire trivial.

– Si $k = 2j - 1$, le réseau de base $(2^{-j}v_1, \ldots, 2^{-j}v_m, 2^{-j}v'_1, \ldots, 2^{-j}v'_m)$, où $v_i := e_i + e_{m+i}$ et $v'_i := e_i - e_{m+i}$, est 2^k-modulaire trivial.

• Supposons $n \equiv 0 \bmod 4$. Soit $(v_1, v_2, \ldots, v_n)$ une base orthogonale et telle que $v_i^2 = 1/4$, et soit R le réseau de base $(v_1, v_2, \ldots, v_n)$ (ainsi, R est 4-modulaire trivial). On définit le sous-groupe Λ_n de R

par la formule

$$\Lambda_n := \left\{ \sum_{i=1}^{i=n} a_i v_i \mid (\forall i,\, a_i \equiv a_1 \bmod 2) \text{ et } \left(\textstyle\sum_i a_i \equiv 0 \bmod 4\right) \right\}.$$

Alors le réseau Λ_n est unimodulaire. Si de plus n est divisible par 8, le réseau Λ_n est pair.

• Le groupe des automorphismes d'un réseau r-modulaire trivial de rang n est isomorphe au groupe des matrices monomiales à coefficients ± 1, groupe isomorphe au produit semi-direct $(\mathrm{Z}/2\mathrm{Z})^n$ o $\mathfrak{S}_n$.

On peut démontrer (cf. [Ser77]) (ceci est à rapprocher du théorème 1.2 ci-dessus) :

3.1. Théorème. *Il existe un réseau unimodulaire pair dans* Q^n *si et seulement si* n *est multiple de* 8.

Réseaux unimodulaires et réseaux 2^k-modulaire triviaux. De la théorie des formes quadratiques entières et de leurs invariants (cf. [O'M00] ou [Ser77], cf. aussi [Bro77], appendice A.2, pour une liste des principaux résultats) on peut déduire le théorème suivant.

3.2. Théorème. *Supposons* $n > 5$. *Pour tout réseau entier* L *de* Q^n, *il existe un entier* k *et un réseau* 2^k*-modulaire trivial* R *tel que*

$$2^k R \subseteq L \subseteq R.$$

Si R est un réseau 2^k-modulaire trivial, ses bases orthogonales formées de vecteurs de carré 2^{-k} définissent toutes le même ensemble de points, noté Ω_R (ou plus simplement Ω) dans $R/2R$. Ainsi, le F_2-espace vectoriel $R/2R$ s'identifie naturellement à $\mathcal{P}(\Omega)$.

Supposons que L est un réseau tel que $2^k R \subseteq L \subseteq R$. Notons que l'on a aussi $2^k R \subseteq L^0 \subseteq R$. La suite ordonnée de réseaux

$$L \subset 2^{-1}L \subset 2^{-2}L \subset \cdots \subset 2^{k-1}L \subset 2^{-k}L$$

donne, par intersection avec R, puis par réduction modulo $2R$, une suite de codes dans $\mathcal{P}(\Omega)$:

$$\mathcal{E}_0(L) \subseteq \mathcal{E}_1(L) \subseteq \mathcal{E}_2(L) \subseteq \cdots \subseteq \mathcal{E}_{k-1}(L) \subseteq \mathcal{P}(\Omega).$$

La proposition suivante relie orthogonalité des codes et duaux des réseaux. On y utilise les notations qui précèdent.

3.3. Proposition. *Pour tout entier j ($1 \leq j \leq k-1$), on a*

$$\mathcal{E}_j(L)^0 = \mathcal{E}_{k-1-j}(L^0).$$

Premier exemple

• On a défini, pour n multiple de 4, le réseau unimodulaire Λ_n dans $\mathbb{Q}^n$ comme sous-groupe d'un réseau 4-modulaire trivial R. Ainsi on a $4R \subset \Lambda_n \subset R$. La suite de codes correspondante dans $\mathcal{P}(\Omega)$ est $\mathcal{D}(\Omega) \subset \mathcal{H}(\Omega)$.

• Posons $n = 2m$. Si $(v_1, v_2, \ldots, v_n)$ est une base orthogonale de R avec $v_i^2 = 1/4$, on note T le réseau 2-modulaire trivial de base

$$(w_1, \ldots, w_m, w'_1, \ldots, w'_m),$$

où $w_i := v_i + v_{i+m}$ et $w'_i := v_i - v_{i+m}$. On voit que $2T \subset L \subset T$. Comme L est unimodulaire, ceci définit un code auto-orthogonal dans $\mathcal{P}(\Omega_T)$. C'est le code engendré par les éléments de la forme $\{i, j, i+m, j+m\}$ pour $1 \leq i, j \leq m$ et $i \neq j$.

Fonction thêta d'un réseau. Soit L un réseau de $\mathbb{Q}^n$. Sa fonction thêta est par définition la fonction définie sur le demi-plan de Poincaré $\{\zeta \in \mathbb{C} \mid (\mathrm{im}(z) > 0)\}$ par

$$\Theta_L(z) := \sum_{x \in L} e^{\pi i x^2 z}.$$

En particulier, si L est pair, on pose $q := e^{2\pi i z}$ et on a

$$\Theta_L(z) = \sum_{r>0} |L_{2r}|\, q^r,$$

où on désigne par L_{2r} l'ensemble de vecteurs de L de carré $2r$.

Exemple. On définit une fonction de $\mathbb{N}$ dans $\mathbb{N}$ par la formule

$$\sigma_3(r) := \sum_{\{d \mid (d \mid r)\}} d^3.$$

La fonction thêta du réseau Λ_8 défini ci-dessus, notée $\Theta_8(z)$, est

$$\Theta_8(z) = 1 + 240 \sum_{r>1} \sigma_3(r) q^r = 1 + 240q + 2160q^2 + 6720q^3 + \cdots .$$

La fonction thêta est l'analogue pour les réseaux du polynôme des poids d'un code. On a par exemple l'analogue suivant de la formule de Mac Williams, la *formule de Poisson*.

3.4. Théorème. *Supposons $n = 2m$, où m est un entier. Pour tout réseau L de $\mathbb{Q}^n$, on a*

$$\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z).$$

De même que pour les codes auto-orthogonaux pairs, on en déduit une propriété d'invariance des fonctions thêta des réseaux unimodulaires pairs, d'où leur appartenance à un espace vectoriel de dimension finie.

Formes modulaires

Une *forme modulaire de degré n* (cf. [Ser77]) est une fonction θ holomorphe sur le demi-plan de Poincaré, vérifiant les propriétés suivantes.

(m1) *Invariance* : $\theta(z+1) = \theta(z)$ et $\theta(z) = z^n\theta(-1/z)$.

(m2) *Holomorphie aux pointes* : Si $\theta(z) = \sum_{r>0} a_r q^r$ est le développement en série de Fourier de θ, il existe un nombre réel $c > 0$ tel que $a_r = \mathrm{O}(r^c)$.

On dit que la forme θ est *à coefficients entiers* si ses coefficients de Fourier a_r sont entiers.

On définit une forme modulaire de poids 24 (la « fonction de Ramanujan ») par la formule

$$\Delta(z) := q\prod_{n>1}(1-q^n)^{24}.$$

On démontre alors que l'espace vectoriel des formes modulaires est l'algèbre engendrée par les deux éléments Θ_8 et Δ. Il en résulte

3.5. Proposition. *La dimension de l'espace vectoriel des formes modulaires de degré n est $1 + \left[\dfrac{n}{24}\right]$.*

Plus précisément, la Z-algèbre des formes modulaires à coefficients entiers est engendrée par les deux fonctions Θ_8 et Δ.

Application aux fonctions thêta

La fonction thêta d'un réseau unimodulaire pair est une forme modulaire de degré n à coe□cients entiers. Comme le terme constant d'une fonction thêta est égal à 1, on en déduit en particulier

3.6. Proposition

(1) *Il y a une seule fonction qui peut être la fonction thêta d'un réseau unimodulaire pair en dimension* 8*, à savoir la fonction* Θ_8*.*

(2) *Il y a une seule fonction qui peut être la fonction thêta d'un réseau unimodulaire pair en dimension* 24 *ne contenant aucun vecteur de carré* 2*.*

Notons Θ_{24} la fonction définie dans l'assertion (2) de la proposition précédente. On a

$$\Theta_{24} = 1 + 196560\,q^2 + 16773120\,q^3 + 398034000\,q^4 + \cdots .$$

Nous allons voir qu'il existe e□ectivement un réseau unimodulaire pair en dimension 24 ne contenant aucun vecteur de carré 2, le *réseau de Leech*. il est construit à l'aide du code orthogonal pair en dimension 24 invariant par M_{24} et son groupe d'automorphismes est le *groupe de Conway*.

4. Le réseau Λ_8 et le réseau de Leech

Sur le réseau de Leech et son groupe d'automorphismes

Soit $(v_1, v_2, \ldots, v_{24})$ une base orthogonale de Q^{24} faite de vecteurs de carré $1/8$. Soit R le réseau engendré par cette base, et soit Ω l'image de la base dans $R/2R$; on identifie Ω à $\{1, 2, \ldots, 24\}$. Pour $X \subseteq \Omega$, on pose $v_X := \sum_{i\in X} v_i$, et on note ε_X l'automorphisme de R défini par

$$\varepsilon_X(v_i) = \begin{cases} -v_i & \text{si } i \in X, \\ \ \ v_i & \text{si } i \in X. \end{cases}$$

On note $\mathcal{E}$ le code auto-orthogonal pair dans $\mathcal{P}(\Omega)$ engendré par les cellules d'un système de Steiner de type $\mathrm{St}(5, 8, 24)$, qui constituent l'ensemble $\mathcal{E}_8$ des éléments de poids 8 de $\mathcal{E}$.

Définition. On appelle *réseau de Leech* et on note Λ_{24} l'ensemble des vecteurs $x = \sum_{1 \leqslant i \leqslant 24} x_i\, v_i$, où

- les x_i sont entiers et tous de même parité,
- pour tout $a \in \mathbb{Z}/4\mathbb{Z}$, $\{i \mid (x_i \equiv a \bmod 4)\} \in \mathcal{E}$,
- $\sum_{1 \leqslant i \leqslant 24} x_i \equiv 4x_1 \bmod 8$.

Il n'est pas difficile de voir que l'inclusion $8R \subset \Lambda_{24} \subset R$ fournit dans $\mathcal{P}(\Omega)$ la suite de codes

$$\mathcal{E}_0(\Lambda_{24}) = \mathcal{D}(\Omega) \subset \mathcal{E}_1(\Lambda_{24}) = \mathcal{E} \subset \mathcal{E}_2(\Lambda_{24}) = \mathcal{H}(\Omega),$$

et que Λ_{24} est engendré par le système de vecteurs suivants :

$$\{8v_i,\ 4v_i - 4v_j,\ 2v_C,\ v_\Omega - 4v_i\}_{(1 \leqslant i,j \leqslant 24),(C \in \mathcal{E}_8)}.$$

Le réseau de Leech est unimodulaire pair, et il ne contient pas de vecteur de carré 2. Sa fonction thêta est donc la fonction Θ_{24} définie au paragraphe précédent.

L'ensemble des vecteurs de Λ_{24} de carré 4 est constitué de l'union des ensembles de vecteurs suivants :

$$\begin{cases} \{\pm 4v_i \pm 4v_j\}_{i \neq j}, \\ \{2\varepsilon_X(v_C) \mid (\langle X, C\rangle = 0)(C \in \mathcal{E}_8)\}, \\ \{\varepsilon_E(v_\Omega - 4v_i) \mid (E \in \mathcal{E})\}. \end{cases}$$

On démontre que le groupe des automorphismes de Λ_{24} est transitif sur l'ensemble des vecteurs de carré 4. On l'appelle *le groupe de Conway*, il est d'ordre

$$2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23,$$

et son quotient par son centre $\{\pm 1\}$ est un groupe simple sporadique.

Remarque. Après avoir constaté que le plus grand nombre premier qui divise l'ordre du groupe de Conway est 23, on se reportera à l'appendice ci-dessous sur les éléments d'ordre fini dans $\mathrm{GL}_n(\mathbb{Q})$.

Afin de donner au lecteur une première idée des méthodes nécessaires pour démontrer les résultats précédents, nous présentons ci-dessous une esquisse d'étude du groupe des automorphismes du réseau Λ_8 qui, par bien des aspects, est une « version simplifiée » du réseau de Leech.

Le réseau Λ_8 et son groupe d'automorphismes

Premières propriétés

Soit $(v_1, v_2, \ldots, v_8)$ une base orthogonale de $\mathbb{Q}^8$ faite de vecteurs de carré $1/4$. Soit R le réseau engendré par cette base, et soit Ω l'image de la base dans $R/2R$; on identifie Ω à $\{1, 2, \ldots, 8\}$. Pour $X \subseteq \Omega$, on pose $v_X := \sum_{i \in X} v_i$, et on note ε_X l'automorphisme de R défini par

$$\varepsilon_X(v_i) = \begin{cases} -v_i & \text{si } i \notin X, \\ v_i & \text{si } i \in X. \end{cases}$$

Rappelons que le réseau Λ_8 (dorénavant noté Λ) est le réseau unimodulaire pair constitué des vecteurs $x = \sum_{1 \leqslant i \leqslant 8} x_i\, v_i$, tels que

- les x_i sont entiers et tous de même parité,
- $\sum_{1 \leqslant i \leqslant 8} x_i \equiv 0 \bmod 4$.

On sait que les inclusions $4R \subset \Lambda \subset R$ fournissent dans $\mathcal{P}(\Omega)$ la suite de codes

$$\mathcal{E}_0(\Lambda) = \mathcal{D}(\Omega) \subset \mathcal{E}_1(\Lambda) = \mathcal{H}(\Omega).$$

D'autre part, il est facile de voir que Λ est engendré par le système de vecteurs suivants :

$$\{4v_i,\ 2v_i - 2v_j,\ v_\Omega\}_{(1 \leqslant i,j \leqslant 8)},$$

et que l'ensemble $\Lambda(2)$ des « petits vecteurs » de Λ (i.e., l'ensemble des vecteurs de carré 2) est

$$\Lambda(2) = \{\pm 2v_i \pm 2v_j \mid (i \neq j)\} \ \cup\ \{\varepsilon_H(v_\Omega) \mid (H \in \mathcal{H}(\Omega))\}.$$

Sur les automorphismes

L'application $\mathcal{P}(\Omega) \to \mathrm{GL}_8(\mathbb{Q}),\ X \mapsto \varepsilon_X$ est un morphisme injectif de groupes. On note $\mathfrak{E}$ l'image de $\mathcal{P}(\Omega)$ par ce morphisme. Plus généralement, pour tout sous-espace $\mathcal{E}$ de $\mathcal{P}(\Omega)$, on note $\mathfrak{E}_\mathcal{E}$ l'image de $\mathfrak{E}$.

Pour $g \in \mathfrak{S}_\Omega$, on note encore g l'automorphisme de $\mathbb{Q}^n$ défini par $g(v_i) := v_{g(i)}$.

Pour $X \subseteq \Omega$ et $g \in \mathfrak{S}_\Omega$, on a $g\varepsilon_X g^{-1} = \varepsilon_{g(X)}$, et le groupe $\mathrm{Aut}(R)$ des automorphismes de R est isomorphe au produit semi-direct $\mathfrak{E} \circ \mathfrak{S}_\Omega$.

On pose $N := \mathrm{Aut}(\Lambda) \cap \mathrm{Aut}(R)$.

4.1. Lemme

(1) *On a* $N = \mathfrak{E}_{\mathcal{H}(\Omega)} \rtimes \mathfrak{S}_\Omega$.

(2) *Si* η *est la symétrie par rapport à* v_Ω, *on a* $\eta \in G\text{–}N$.

Démonstration. Démontrons la deuxième assertion. On a $\eta(v_i) = v_i - (1/4)v_\Omega$. On voit donc que

$$\begin{cases} \eta(4v_i) = 4v_i - v_\Omega, \\ \eta(2v_i - 2v_j) = 2v_i - 2v_j, \\ \eta(v_\Omega) = -v_\Omega, \end{cases}$$

donc que η stabilise Λ.

Soit H un sous-groupe de $\mathrm{Aut}(\Lambda)$ qui contient strictement N.

1. Le groupe H est transitif sur $\Lambda(2)$.

Le groupe N a deux orbites sur l'ensemble des petits vecteurs de Λ, à savoir les ensembles

$$\Gamma_1 := \{\varepsilon_H(v_\Omega)\}_{H \in \mathcal{H}(\Omega)} \quad \text{et} \quad \Gamma_2 := \{\pm 2v_i \pm 2v_j\}_{i \neq j}.$$

Il n'est pas di□cile de vérifier que si un élément du groupe orthogonal de $\mathbb{Q}^n$ stabilise l'ensemble Γ_2, il appartient à $\mathrm{Aut}(R)$. Il en résulte bien que H est transitif sur $\Lambda(2)$.

2. Pour tout $v \in \Lambda(2)$, le stabilisateur H_v de v est transitif sur l'ensemble $\Lambda(2, v)$ des petits vecteurs de Λ qui sont orthogonaux à v.

Soit $v := 2v_1 + 2v_2$. Alors les orbites du stabilisateur N_v de v dans $\Lambda(2, v)$ sont les ensembles

$$\begin{cases} P_0 := \{\pm(2v_1 - 2v_2)\}, \text{ de cardinal } 2, \\ P_1 := \{\varepsilon_H(\Omega) \mid (H \cap \{1,2\} = \text{?})\}, \text{ de cardinal } 2^6 \equiv 1 \bmod 7, \\ P_2 := \{\pm 2v_i \pm 2v_j \mid (\{i,j\} \cap \{1,2\} = \text{?}))\}, \text{ de cardinal } 2^2 \binom{6}{4} \equiv 4 \bmod 7. \end{cases}$$

Il su□t de démontrer que toutes les orbites de H_v sur $\Lambda(2, v)$ sont de cardinal divisible par 7, car alors on voit qu'il ne peut y avoir qu'une seule orbite. Comme H est transitif sur $\Lambda(2)$, on peut remplacer v par l'unique point fixe dans $\Lambda(2)$ d'un élément α d'ordre 7 de N, à savoir v_Ω. Dans ce cas, comme α n'a pas de point fixe, toutes ses orbites non réduites à $\{v_\Omega\}$ sont de cardinal divisible par 7, et il en est de même pour les orbites de H_{v_Ω}.

3. Les seuls vecteurs de Λ de carré 6 4 qui sont équivalents à $4v_i$ (resp. $2v_1 - 2v_2$) modulo 2Λ sont les $\pm 4v_i$ (resp. $\pm(2v_1 - 2v_2)$).

En effet, un calcul facile montre que si deux vecteurs de carré 6 4, distincts et non opposés, sont équivalents modulo 2Λ, alors ils sont orthogonaux et tous deux de carré 4.

4. Le sous-groupe N est maximal dans $\mathrm{Aut}(\Lambda)$ et on a $|\mathrm{Aut}(\Lambda)| = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$.

Il suffit de démontrer que H est d'ordre $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$. Soient $v := 2v_1 + 2v_2$ et $v' := 2v_1 - 2v_2$. Le stabilisateur $H_{v,v'} = H_v \cap H_{v'}$ du couple (v, v') dans H fixe $4v_1$. D'après 4, on voit que $H_{v,v'}$ est contenu dans N, ce que nous notons $H_{v,v'} = N_{v,v'}$.

Par les propriétés de transitivité démontrées ci-dessus (cf. 4 et 4), on voit donc que

$$|H| = |\Lambda(2)| \cdot |\Lambda(2, v)| \cdot |N_{v,v'}|,$$

d'où le résultat annoncé.

5.... Nous renvoyons le lecteur à la littérature pour démontrer que le groupe $\mathrm{Aut}(\Lambda)/\{\pm 1\}$ a un sous-groupe simple d'indice 2.

On peut d'ailleurs démontrer que le groupe $\mathrm{Aut}(\Lambda)/\{\pm 1\}$ opère fidèlement sur le $\mathbf{F}_2$-espace vectoriel $\Lambda/2\Lambda$ en y préservant la forme quadratique qui y est définie par la réduction modulo 2 de $x^2/2$, et en déduire que $\mathrm{Aut}(\Lambda)/\{\pm 1\}$ est isomorphe au groupe orthogonal $\mathrm{O}_8(\mathbf{F}_2)$.

Appendice : Éléments d'ordre fini de $\mathrm{GL}_n(\mathbf{Q})$

4.2. Proposition

(1) *Supposons que l'entier m est l'ordre d'un élément de $\mathrm{GL}_n(\mathbf{Q})$. Il existe un entier s et s entiers distincts $d_1, d_2, \ldots, d_s$ tels que*

- $m = \mathrm{ppcm}\{d_1, d_2, \ldots, d_s\}$,
- $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_s) \leq n$.

(2) *Soient $p_1, p_2, \ldots, p_r$ des nombres premiers distincts. Si $\mathrm{GL}_n(\mathbf{Q})$ a un élément d'ordre $p_1 p_2 \cdots p_r$, on a $p_1 + p_2 + \cdots + p_r \leq n + r$.*

(3) *Si p est un nombre premier qui divise l'ordre d'un sous-groupe fini de $\mathrm{GL}_n(\mathbf{Q})$, on a $p \leq n + 1$.*

Démonstration de 4.2.

(1) Pour tout entier d, on note $\Phi_d(X)$ le d-ième polynôme cyclotomique.

Soit g un élément de $\mathrm{GL}_n(\mathbf{Q})$ d'ordre m et soit $\mu(X)$ le polynôme minimal de g. Comme $\mu(X)$ divise $X^m - 1$ et que $\mu(X) = \prod_{d|m} \Phi_d(X)$,

il existe une famille $d_1, d_2, \ldots, d_s$ de diviseurs distincts de m tels que $\mu(X) = \Phi_{d_1}(X)\Phi_{d_2}(X)\cdots\Phi_{d_s}(X)$.

Soit $m' := \mathrm{ppcm}\{d_1, d_2, \ldots, d_s\}$. Comme $\mu(X)$ divise $X^{m'} - 1$, on voit que $m' = m$.

Comme $\deg \mu(X)$ 6 n on voit que $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_s)$ 6 n.

(2) Posons $m = p_1 p_2 \cdots p_r$. Si $d_1, d_2, \ldots, d_s$ sont tels que

$$m = \mathrm{ppcm}\{d_1, d_2, \ldots, d_s\},$$

chaque d_j est produit d'un certain nombre des p_i, et tout p_i divise au moins l'un des d_j, d'où il résulte que

$$\varphi(p_1) + \varphi(p_2) + \cdots + \varphi(p_r) \text{ 6 } \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_s),$$

et grâce à l'assertion (1) on voit que $\varphi(p_1)+\varphi(p_2)+\cdots+\varphi(p_r)$ 6 n, d'où (2).

(3) est une conséquence immédiate de (2) et du fait que si p divise l'ordre d'un groupe fini, ce groupe fini contient un élément d'ordre p.

Références

[Bou68] N. Bourbaki – *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV : Groupes de Coxeter et systèmes de Tits. Chapitre V : Groupes engendrés par des réflexions. Chapitre VI : systèmes de racines*, Actualités Scientifiques et Industrielles, vol. 1337, Hermann, Paris, 1968.

[Bro77] M. Broué – « Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant $+1$ », *Discrete Math.* **17** (1977), no. 3, p. 247–269.

[Con69a] J. H. Conway – « A characterisation of Leech's lattice », *Invent. Math.* **7** (1969), p. 137–142.

[Con69b] ———, « A group of order $8,315,553,613,086,720,000$ », *Bull. London Math. Soc.* **1** (1969), p. 79–88.

[CS99] J. H. Conway & N. J. A. Sloane – *Sphere packings, lattices and groups*, 3e éd., Grundlehren Math. Wissen., vol. 290, Springer-Verlag, New York, 1999.

[Mat73] É. Mathieu – « Sur la fonction cinq fois transitive de 24 quantités », *J. Math. Pures Appl.* **18** (1873), p. 25–46.

[O'M00] O. T. O'Meara – *Introduction to quadratic forms*, Classics in Math., Springer-Verlag, Berlin, 2000.

[Ser77] J.-P. Serre – *Cours d'arithmétique*, 2e éd., Le Mathématicien, vol. 2, Presses Universitaires de France, Paris, 1977.

[Wit37] E. Witt – « Über Steinersche Systeme », *Abh. Math. Sem. Univ. Hamburg* **12** (1937), no. 1, p. 265–275.

Michel Broué, Institut Henri-Poincaré, 11 rue Pierre et Marie Curie, F-75231 Paris Cedex 05, France

E-mail : broue@math.univ-paris-diderot.fr

Url : https://webusers.imj-prg.fr/~michel.broue/