Système de Steiner S(5,6,12) et Action de $\mathrm{PSL}_2(\mathbb{F}_p)$ sur p points

Jacques Folléas

17 juin 2015

Introduction

Je me suis, dans un premier temps, intéressé aux systèmes de Steiner et à la théorie des codes correcteurs, en particulier aux codes de Golay. Je me suis demandé comment construire un ensemble de points vérifiant des propriétés semblables aux systèmes de Steiner. Cela intervient lorsque l'on recherche un code parfait comme les codes de Hamming, de Golay 11 et de Golay 24, utilisés pour la transmistion des message par la NASA. Le postulat de Galois semblait lié car le groupe $\mathrm{PSL}_2(\mathbb{F}_p)$ agit sur les $p+1$ points de la droite projective. Une idée naturelle pour définir une action sur p points consiste à faire, d'une façon ou d'une autre, des "paquets". Les premmiers groupes étant trop petits pour que les calculs soient intéressants, j'ai commencé avec 5 points. Le but était de me familiariser avec la géométrie projective sur un corp fini et de trouver des techniques afin de pouvoir en tirer des appliquations et des extentions aux systhèmes de Steiners et aux groupes de Mathieu, comme montrer que $\mathrm{PSL}_2(\mathbb{F}_{11})$ pouvait être injecté dans le groupe de Mathieu M_{12}, groupe de symétries du $S(5,6,12)$, dont on ademettera l'unicité. Et par la même occasion de trouver une une façon non trivial de construire un tel système de Steiner, qui permet d'obtenir le code ternaire de Golay G_{11}.

1 Préliminaires de géométrie projective

Pour montrer des isomorphismes entre $\mathrm{PSL}_2(\mathbb{F}_p)$ et les groupes des symétries d'un ensemble de p points, nous aurrons besoins d'un certain nombre d'outils et de quelques propriétés qui vont de pair.

1.1 Droite projective, symétries, homographie, invarience et birapport

Commençons par décrire notre support de travail. Soit $\mathbb{F}_p$ un corps fini à p éléments où p est un nombre premier impair. On note :

$$\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}\ ,\ \mathrm{PGL}_2(\mathbb{F}_p) = \{h_A : z \mapsto \frac{az+b}{cz+d} | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)\}$$

$$\text{et } \mathrm{PSL}_2(\mathbb{F}_p) = \{h_A : z \mapsto \frac{az+b}{cz+d} | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)\}$$

.

On montre alors par un calcul simple que $\mathrm{PGL}_2(\mathbb{F}_p)$ est un goupe sous l'action de composition.

Dans toute la suite de cette partie les $(z_i)_{i\in\mathbb{N}}$ seront des points de $\mathbb{P}^1(\mathbb{K})$ distincts.

L'une des propriétés remarquables de ce groupe est que l'on peut lui exercer un certain contrôle. Cela est illustré par le lemme suivant.

Lemme 1. *Pour toute paire de triplet $(z_1; z_2; z_3)$, $(z'_1; z'_2; z'_1)$ tel que $z_1 \neq z_2 \neq z_3 \neq z_1$ et $z'_1 \neq z'_2 \neq z'_3 \neq z'_1$ dans $\mathbb{F}_p$, il existe $h \in \mathrm{PGL}_2(\mathbb{F}_p)$ tel que $h(z_1)=z'_1$, $h(z_2)=z'_2$ et $h(z_3)=z'_3$.*

On dit alors que $\mathrm{PGL}_2(\mathbb{F}_p)$ est trois fois transitif sur $\mathbb{P}^1(\mathbb{F}_p)$.

Posons $h \in \mathrm{PGL}_2(\mathbb{F}_p)$ tel que $h(\mathrm{z}_1)=\infty$, $h(\mathrm{z}_2)=0$, et $\mathrm{h}(z_3)=1$. On appelle alors *birapport* du quadruplet $(\mathrm{z}_1, z_2, z_3, z_4)$ dont les éléments sont distincts deux à deux et on le note :

$$[z_1, z_2, z_3, z_4] = h(z_4).$$

On a également $h(z_4) \in \mathbb{P}^1(\mathbb{F}_p)\backslash\{0;1;\infty\}$ puisque z_4 est distinct des z_1, z_2, et z_3.

Par un calcul direct on peut montrer que pour tout $k \in \mathrm{PGL}_2(\mathbb{F}_p)$ et pour tout (z_1, z_2, z_3, z_4),

$$[k(z_1), k(z_2), k(z_3), k(z_4)] = [z_1, z_2, z_3, z_4].$$

En exploitant la formule du lemme 1 $[z_1, z_2, z_3, z_4] = \frac{(z_3-z_1)(z_4-z_2)}{(z_3-z_2)(z_4-z_1)}$ on montre alors que :

$$[z_1, z_2, z_3, z_4] = [z_2, z_1, z_4, z_3] = [z_3, z_4, z_1, z_2] = [z_4, z_3, z_2, z_1] = [z_2, z_1, z_3, z_4]^{-1}. \qquad (*)$$

Mais également que :

$$[z_1, z_2, z_3, z_4] + [z_1, z_3, z_2, z_4] = [z_1, z_2, z_3, z_4] + [z_4, z_2, z_3, z_1] = 1.$$

Remarque. On peut alors voir grâce à (*) que le birapport de quatre points peut prendre au plus six valeurs ($\frac{4!}{4}$).

1.2 Conjugué harmonique, équianharmonique et chevauchement

Définissons quelques notions qualifiants un quadruplet de $\mathbb{P}^1(\mathbb{F}_p)$.

Soit(z_1, z_2, z_3, z_4). On dit que z_2 est le *conjugué harmonique* de z_1 par z_3 et z_4 si $[z_1, z_2, z_3, z_4] = -1$. On parle alors de quadruplet harmonique lorsque le birapport du quadruplet est dans $\{-1, 2, 1/2\}$.

Enfin, si un quadruplet est formé de deux paires harmoniquement conjuguées, il existe deux partitions en deux paires de ce quadruplet tel que les deux paires ne soient pas harmoniquement conjuguées. On dira alors que cette partition *chevauche* [1] le quadruplet.

Remarque. Si l'on fixe trois points (z_1, z_3, z_4) alors il existe un unique z_2 tel que z_2 soit le conjugué harmonique de z_1 par z_3 et z_4 : $z_2 = (z_4 + z_3\frac{z_3-z_1}{z_4-z_1})(1 + \frac{z_3-z_1}{z_4-z_1})^{-1}$.

Fixons z_1 et z_2 des éléments de $\mathbb{F}_p$, et considérons l'application $\Gamma_{z_1,z_2} : z \longmapsto z'$ tel que $[z_1, z_2, z, z'] = -1$.

Lemme 2. *L'application $\Gamma_{1,2}$ n'admet que deux points fixes : z_1 et z_2.*

Démonstration. En effet, par quelques calculs sans grande subtilités on trouve :

$$\Gamma(z) = z' = \frac{(z_1 + z_2)z - 2z_1z_2}{2z - (z_1 + z_2)}.$$

De même par un calcul direct, on montre que les points fixes de cette application $\Gamma_{1,2}$ sont les racines du polynôme $X^2 - (z_1 + z_2)X + z_1z_2$, soit z_1 et z_2. □

De même, on dit qu'un quadruplet $\{z_1,z_2,z_3,z_4\} \in \mathbb{P}^1(\mathbb{F}_p)$ est *équianharmonique* si le birapport $[z_1,z_2,z_3,z_4]$ est dans $\{-j,-j^2\}$, où j est racine cubique de l'unité différente de 1 [2]. Le birapport ne peut alors prendre que ces deux valeurs.

1.3 Quelques théorèmes importants sur les groupes

Rappelons dans un premier temps le théorème élémentaire suivant.

Théorème 1. *Soit G un groupe fini agissant sur X, et $x \in X$, si l'on note $Stab_G(x)$ le stabilisateur de x sous l'action de G et $Orb_G(x)$ l'orbite de x, alors on a $|G| = |Orb_G(x)| \times |Stab_G(x)|$.*

Nous aurons également besoin de théorèmes plus puissants.

1. straddle en anglais
2. N.B. : Ceci n'existe que si $p \equiv 1(p)$

Cauchy et Sylow

Théorème 2. *(de Cauchy) Soit G un groupe fini et p un diviseur premier de l'ordre n de G. Alors il existe dans G au moins un élément d'ordre p.*

Soit un groupe G, tel que $|G| = p^\alpha m$ avec $p \nmid m$, on définit p-sous-groupe de Sylow ou p-Sylow de G un sous groupe de cardinal p^α.

Théorème 3. *Soit G un groupe fini et p un diviseur premier de $|G|$ alors G contient au moins un p-sous-groupe de Sylow ou p-Sylow de G un sous-groupe de cardinal p^α.*

Théorème 4. *Soit un groupe G, tel que $|G| = p^\alpha m = n$ avec $p \nmid m$.*
(i) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S, avec $H \subset S$.
(ii) Les p-Sylows sont tous conjugués et donc leur nombre k divise n.
(iii) $k \equiv 1(p)$ donc k divise m.

Nous admetrons ces théorèmes dont la démonstration est dans Algèbre Théorie des groupes de Anne Cortella à la page 57.

Proposition 1. *Le groupe symétrique $\mathfrak{S}_n$ a un unique sous-groupe H d'indice 2 qui est le groupe alterné $\mathfrak{A}_n$.* [3]

1.4 Calcul de cardinaux sur un corps fini $\mathbb{F}_p$

En considérant les bases de $\mathbb{F}_p^2$ et les matrices dont le déterminant est un carré, on trouve par un calcul simple que $|\operatorname{PGL}_2(\mathbb{F}_p)| = \frac{|\operatorname{GL}_2(\mathbb{F}_p)|}{|\mathbb{F}_p^*|} = (p^3 - p)$ et que $|\operatorname{PSL}_2(\mathbb{F}_p)| = \frac{|\operatorname{PGL}_2(\mathbb{F}_p)|}{2} = \frac{p^3-p}{2}$.

2 Action de $\operatorname{PSL}_2(\mathbb{F}_p)$ sur p points et isomorphismes exeptionnels

2.1 Synthèmes harmoniques sur $\mathbb{F}_5$

Commençons par définir notre environnement de travail. Après avoir fixé $p = 5$ montrons le lemme suivant.

Lemme 3. *En fixant z_5 et z_6 dans $\mathbb{P}^1(\mathbb{F}_5)$, on peut alors ordonner les quatre points restants de $\mathbb{P}^1(\mathbb{F}_5)$ en une famille (z_1, z_2, z_3, z_4) tel que $[z_1, z_2, z_3, z_4] = -1$. De plus z_5 est le conjugué harmonique de z_6 par z_3 et z_4 et également par z_1 et z_2.*

La démonstration est relativement simple par élimination des possibilités et apporte peu à ce mémoire. [4] On dira alors que les paires $\{z_1, z_2\}$, $\{z_3, z_4\}$ et $\{z_5, z_6\}$ sont *harmoniquement séparées* et que la partition $\big\{\{z_1, z_2\}; \{z_3, z_4\}; \{z_5, z_6\}\big\}$ forme un synthème harmonique. Par conservation du birapport, l'image d'un synthème par homographie est un synthème.

Les synthèmes harmoniques seront alors les points sur lesquels nous ferons agir $\operatorname{PGL}_2(\mathbb{F}_5)$ et $\operatorname{PSL}_2(\mathbb{F}_5)$.

Comptons alors les synthèmes harmoniques. Rappelons-nous qu'un synthème harmonique est déterminé par une paire de points de $\mathbb{P}^1(\mathbb{F}_5)$. Tous les points de $\mathbb{P}^1(\mathbb{F}_5)$ appartiennent à une et une seule paire de chaque synthème. Comme $\operatorname{PSL}_2(\mathbb{F}_5)$ est transitif sur $\mathbb{P}^1(\mathbb{F}_5)$, on peut alors choisir sans perte de généralité $z_1 = \infty$ ce qui laisse seulement cinq possibilités pour le deuxième point, il n'y a donc que 5 synthèmes harmoniques distincts.

Remarque. On peut également remarquer par cardinalité que toute paire d'éléments de $\mathbb{P}^1(\mathbb{F}_5)$ est contenu dans un unique synthème (ce qui nous rappelle les systèmes de Steiner). En effet un synthème étant uniquement déterminé par une paire d'éléments de $\mathbb{P}^1(\mathbb{F}_5)$ si une paire est commune à deux synthèmes ces derniers sont égaux, et il y a cinq sythèmes soit quinze paires d'éléments de $\mathbb{P}^1(\mathbb{F}_5)$. Or $15 = \binom{6}{2}$, ce qui conclut la remarque.

3. Voir démonstration en annexe.
4. Vous la trouverez toutefois en annexe.

Il faut ensuite définir l'action de $\mathrm{PGL}_2(\mathbb{F}_5)$ sur l'ensemble des synthèmes que nous noterons dorénavant $\mathscr{S}$. On définit alors le morphisme $\iota : \mathrm{PGL}_2(\mathbb{F}_5) \mapsto \mathfrak{S}_{\mathscr{S}}$ tel que, soit $h \in \mathrm{PGL}_2(\mathbb{F}_5)$ et $s_1 = \{\{z_1, z_2\}; \{z_3, z_4\}; \{z_5, z_6\}\} \in S$, on a l'application

$$\iota(h) = \tilde{h} : \mathscr{S} \mapsto \mathscr{S} \text{ tel que } \tilde{h}(S_1) = \big\{\{h(z_1), h(z_2)\}; \{h(z_3), h(z_4)\}; \{h(z_5), h(z_6)\}\big\}.$$

Cette action est bien définie par invariance du birapport par homographie. Cela permet alors d'injecter le groupe $\mathrm{PGL}_2(\mathbb{F}_5)$ dans $\mathfrak{S}_{\mathscr{S}}$. Un synthème est uniquement déterminée par une paire d'éléments de $\mathbb{P}^1(\mathbb{F}_5)$. La triple transitivité de $\mathrm{PGL}_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$, nous donne alors le résultat suivant.

Lemme 4. *L'action induite par* $\mathrm{PGL}_2(\mathbb{F}_5)$ *est transitive sur* $\mathscr{S}$.

Lemme 5. *L'action induite par* $\mathrm{PGL}_2(\mathbb{F}_5)$ *sur* $\mathscr{S}$ *est fidèle.*

Démonstration. [5] La démonstration consiste à utiliser la simplicité du groupe $PSL_2(\mathbb{F}_5)$ dont la démonstration est non triviale. Le résultat est en fait vrai pour $PSL_n(\mathbb{F}_k)$ pour tout $n \geq 2$ et $k \geq 2$ avec $(n, k) \neq (2, 2), (2, 3)$. [6]

Supposons un sous-groupe distingué de $PSL_2(\mathbb{F}_k)$, non trivial. Par image réciproque il lui correspond un sous-groupe distingué N de $SL_2(\mathbb{F}_k)$ contenant le centre mais distinct de ce dernier. Et il faut alors montrer que $N = SL_2(\mathbb{F}_k)$. Pour se faire l'idée est d'utiliser un premier élément $\sigma \in N$ distinct du neutre et on fabrique de nouveaux éléments de N, sous forme de commutateurs, en se rappelant $D(SL_n(\mathbb{F}_k)) = SL_n(\mathbb{F}_k)$. [7] Cela nous permet d'affirmer que les seuls sous-groupes distingués de $PGL_2(\mathbb{F}_5)$ sont : $\{e\}$, $PSL_2(\mathbb{F}_5)$, et $PGL_2(\mathbb{F}_5)$ (où e est le neutre de $PGL_2(\mathbb{F}_5)$). Or K, le noyau de l'application ι est distingué. Donc K est stable par automorphisme intérieur. C'est donc l'un des trois sous-groupes $\{e\}$, $PSL_2(\mathbb{F}_5)$, et $PGL_2(\mathbb{F}_5)$. Mais cela ne peut être les deux derniers. En effet si l'on considère les orbites de $PGL_2(\mathbb{F}_5)$ sous K par composition (à gauche) leur nombre est supérieur ou égale à $5 > |PGL_2(\mathbb{F}_5)/PSL_2(\mathbb{F}_5)| = 2 > |PGL_2(\mathbb{F}_5)/PGL_2(\mathbb{F}_5)| = 1$. Grâce à la transitivité de l'action de $PGL_2(\mathbb{F}_5)$. Par élimination, en appliquant le théorème 1, K n'est autre que e. D'où la fidélité de l'action. □

Enfin sachant que les deux groupes sont de même cardinal, on en déduit l'isomorphisme entre $\mathrm{PGL}_2(\mathbb{F}_5)$ et $\mathfrak{S}_S$ et donc entre $\mathrm{PGL}_2(\mathbb{F}_5)$ et $\mathfrak{S}_5$. En effet en numérotant les synthèmes de 1 à 5 on a un isomorphisme $f : \mathfrak{S}_s \mapsto \mathfrak{S}_5$ et la composée $f \circ \iota$ est l'isomorphisme entre $\mathrm{PGL}_2(\mathbb{F}_5)$, et $\mathfrak{S}_5$.

Caractère exceptionnel de l'isomorphisme : Commençons par énoncer les théorèmes suivants.

Théorème 5. *Pour tout* $n \in \mathbb{N}$, $n \neq 6$, *tout automorphisme de* $\mathfrak{S}_n$ *est intérieur :* $\mathrm{Aut}\mathfrak{S}_n = \mathrm{Int}\mathfrak{S}_n$.

L'isomorphisme fournit alors une preuve que les automorphismes de $\mathfrak{S}_6$ ne sont pas tous intérieurs. En effet comme $|\mathbb{P}^1(\mathbb{F}_5)| = 6$, l'action naturelle de $\mathrm{PGL}_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$ donne une injection $\varphi : PGL_2(\mathbb{F}_5) \longmapsto \mathfrak{S}_6$. Notons alors, $H = \varphi(PGL_2(\mathbb{F}_5))$. Comme H est de cardinal 5! et $\mathfrak{S}_6$ de cardinal 6!, alors le groupe H est d'indice 6 dans $\mathfrak{S}_6$, soit le groupe quotient :

$$X = \mathfrak{S}_6/H = \{eH, g_1H, g_2H, g_3H, g_4H, g_5H\}.$$

Il est de cardinal 6 (pour une famille de $(g_k)_{1\leq k\leq 5}$ convenable et où e est le neutre de $\mathfrak{S}_6$). $\mathfrak{S}_6$ agit alors transitivement sur X, ce qui induit l'existence de l'isomorphisme de groupe

$$\mathbf{\Phi} : \mathfrak{S}_6 \longrightarrow \mathfrak{S}_X \,;\, g \longmapsto \big(\phi(g) : g_kH \longmapsto gg_kH\big).$$

Cet isomorphisme est injectif. En effet, d'une part, comme tout noyau de morphisme de groupe, il est normal ; c'est donc $\{e\}$ ou $\mathfrak{A}_6$ ou $\mathfrak{S}_6$. D'autre part $Ker\mathbf{\Phi} \subset H$ (Si $g \in Ker\mathbf{\Phi}$, $g \cdot eH = eH \Longrightarrow g \in H$).

Or $|H| < |\mathfrak{A}_6| < |\mathfrak{S}_6|$. Donc $Ker\mathbf{\Phi} = \{e\}$. Donc H est envoyé sur le stabilisateur d'un point alors que H agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$. Ce qui prouve que H et $\mathbf{\Phi}(H)$ ne sont pas conjugués dans $\mathfrak{S}_6$ et donc $\mathbf{\Phi}$ n'est pas intérieur comme automorphisme de $\mathfrak{S}_6$.

5. Une démonstration alternative est disponible en annexe.

6. La démonstration est page 113 dans le livre cours d'algèbre de Daniel PERRIN édition 1990.

7. Une démonstration complète de ce postulat se trouve à la page 113 du cours d'algèbre de Daniel PERRIN édition 1990.

Action de $\mathrm{PSL}_2(\mathbb{F}_5)$ sur les synthèmes : Comme nous l'avons montré dans la première partie, $PSL_2(\mathbb{F}_5)$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{F}_5)$. Il en est donc de même pour $\mathscr{S} = f \circ \iota(\mathrm{PSL}_2(\mathbb{F}_5))$ dans $\mathfrak{S}_5$. La proposition 1 nous permet alors de déduire l'isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_5)$ et $\mathfrak{A}_5$, et donc l'action de notre groupe sur 5 points.

2.2 Avec le corps $\mathbb{F}_7$

Le but de cette partie est de montrer que tout groupe simple d'ordre 168 est isomorphe à $PSL_2(\mathbb{F}_7)$. Ce sera alors également le cas pour $PSL_2(\mathbb{F}_3)$. Pour ce faire nous utiliserons deux méthodes. La première utilise principalement la théorie des groupes et l'action non-triviale du groupe sur 8 points qui sont formés des 7-Sylows de ce dernier. La deuxième reprend l'esprit des synthèmes harmoniques et plus en évidence l'action du groupe sur 7 points.

2.2.1 À l'aide du théorème de Sylow

Structure du groupe G : Soit G un groupe simple d'ordre 168.

Montrons alors que les 7-Sylow sont au nombre de 8. Pour cela on commence par utiliser le premier théorème de Sylow, ($168 = 8 \times 3 \times 7$), il existe au moins un 7-Sylow. Notons le S_7 et N_7 le nombre de 7-Sylow. D'après le deuxième théorème de Sylow on a :$N_7 \equiv 1(7)$ ainsi que $N_7 \big| |G|$. Donc $N_7 \in \{1, 8\}$.

Supposons $N_7 = 1$ alors pour tout $g \in G$, $gS_7g^{-1} = S_7$. On a alors $S_7 \lhd G$. Ce qui n'est pas raisonnable puisque cela contredit la simplicité de G. On a alors 8 7-Sylow dans G. Fixons P et Q des éléments de S l'ensemble des 7-Sylows de G. De plus, notons $N = Stab_G(P)$. En désignant par $\omega(P)$ l'orbite de P par action de conjugaison dans G on a alors :

$$8 = |S| = |\omega(P)| = \frac{|G|}{|N|} = \frac{168}{|N|} \text{ donc } |N| = \frac{168}{8} = 21$$

Proposition 2. *Le groupe P opère transitivement sur $S\backslash\{P\}$*

Démonstration. En effet on a $|P| = 7$ donc $P \simeq \mathbb{Z}/7\mathbb{Z}$(si $g \in P\{e\}, \phi : \mathbb{Z} \longrightarrow P; k \longmapsto g^k$, $\phi(\mathbb{Z})$ est un sous-groupe de P de cardinal superieur à 2, donc par cardinalité, $\phi(\mathbb{Z}) = P$). Considérons maintenant le cardinal de l'orbite de $Q \in S\backslash\{P\}$ sous l'action de P par conjugaison, c'est donc un diviseur de $7 = |P|$ et donc c'est 1 ou 7. Supposons que ce soit 1 alors faute de place, tous les points sont conservés par action de P,

$$\text{ie} : \forall g \in P, \forall Q \in S, gQg^{-1} = Q. \qquad (**)$$

Remarquons que si $P, Q \in S, P \cap Q = \{e\}$ ou $P = Q$. En effet $P \cap Q$ est un sous-groupe du groupe P d'ordre 7, c'est donc le groupe tout entier ou $\{e\}$. Donc si on a (**), alors :

$$\forall R \in S, \forall g \in R, \forall Q \in S, gQg^{-1} = Q.$$

En effet, fixons h dans G tel que $hRh^{-1} = P \Leftrightarrow h^{-1}Ph = R$ alors :

$$g \in R, Q \in S : gQg^{-1} = h^{-1}hgh^{-1}hQh^{-1}hg^{-1}h^{-1}h \text{ avec } hgh^{-1} = g' \in P$$

$$\text{et donc par (**) } g'h^{-1}hQh^{-1}hg'^{-1} = hQh^{-1} \text{ donc } g'Qg'^{-1} = Q.$$

Mais ceci n'est pas raisonnable au vu du calcul de $|N|$ que nous avons fait précédemment, on trouverai un nombre d'éléments qui fixe le point $P : 1 + |S| \times 6 = 49 > 21$.

Par conséquent, l'orbite de $Q \in S\backslash\{P\}$ sous l'action de conjugaison dans P est de cardinal 7. □

Nous noterons $N_G(H)$ le normalisateur d'un sous-groupe H dans le groupe G. Considérons maintenant $M := N_G(P) \cap N_G(Q)$ pour P et Q distincts dans S, et montrons la proposition :

Proposition 3. $|M| = 3$.

Démonstration. Commençons par remarquer que $|M|\big||N| = 21$ donc $|M| \in \{1, 3, 7, 21\}$. Supposons dans un premier temps que $7\big||M|$, alors par (i) du Théorème 3, M admet un 7-Sylow qui fixe à la fois P (C'est donc P) et Q (C'est donc Q), ce qui n'a pas beaucoup de sens comme P et Q sont distincts. Donc $|M| \in \{1, 3\}$.

D'après le théorème de Cauchy, N contient au moins un élément n d'ordre 3. De plus comme $3 \nmid 7 = |S\backslash\{P\}|$ l'action de n admet au moins un point fixe sur $S\backslash\{P\}$ car les orbites sous l'action de n sont de cardinal 1 ou 3. Donc : $\exists R \in S\backslash\{P\} : nRn^{-1} = R$. Soit $g \in P$ et k tel que $g^kQg^{-k} = R$ alors $ng^kQg^{-k}n^{-1} = g^kQg^{-k}$, donc $n' = g^{-k}ng^k \in M$. Donc M contient un élément d'ordre 3. Donc $|M| \geq 3$ et donc $|M| = 3$. □

En considérant l'opération de G sur S par conjugaison, on a alors un homomorphisme $\varphi : G \longrightarrow \mathfrak{S}_S$. Montrons alors que ce morphisme est injectif, soit :

$$\text{Si } g \in G \text{ tel que } \forall Q \in S, gQg^{-1} = Q, \text{ alors } g = e.$$

Fixons $g \in Ker(\varphi)\backslash\{e\}$, $g \in M$. De plus par le théorème de Cauchy, g n'étant pas d'ordre 1 et 3 étant premier on en déduit alors que g est d'ordre 3. Par ailleurs, on a $|M| = 3$ donc $M = \langle g\rangle$. $\langle g\rangle$ est alors normal et d'ordre 3 ce qui est absurde, par simplicité de G. Donc le morphisme φ est injectif.

Posons alors $\overline{g} = \varphi(g)$ pour tout $g \in G$. Montrons alors le :

Lemme 6. *Le maximum des ordres d'éléments de $\varphi(G)$ est inférieur à 15.*

Démonstration. Pour démontrer cela, on pose la famille $(\lambda_i)_{i\in I}$ dont les membres sont les ordres des éléments de $\varphi(G)$, où I est un ensemble fini dans $\mathbb{N}$. On a également la famille (λ_i) vérifie : $\big[8 = \sum_I \lambda_i$ et $\lambda_1 \geq \lambda_2 \geq ... \geq 1\ \big]$. Calculons alors le $\text{ppcm}_{i\in I}(\lambda_i)$. En calculant tous les cas pour λ_1 allant de 7 à 1 on trouve que l'ensemble des ordres possibles pour un élément de $\varphi(G)$ est $\{1, 2, 3, 4, 5, 6, 7, 10, 12, 15\}$. □

On en déduit alors que N n'est pas cyclique car $|N| = 21$ et 21 n'est l'ordre d'aucun élément de G puisque $21 > 15$.

Définissons maintenant N_3 le nombre de Sylow d'ordre 3. On a alors par le théorème de Sylow, $N_3 \equiv 1[3]$ et $N_3 \mid \frac{168}{3} = 56$. Donc $N_3 \in \{1, 4, 7, 28\}$. Mais 1 est exclu par simplicité de G. Montrons alors, qu'il y a plus de sept 3-Sylows. Pour cela considérons le nombre de 3-Sylows dans $N = N_G(P)$,pour $P \in S$ fixé, dont le cardinal est 21. Par les théorèmes de Sylow, on sait que le nombre de 3-Sylows de N divise $7 = 21/3$. C'est donc 1 ou 7. On sait déjà que $|N| = 21$ et que N est non cyclique. De plus, toujours par le théorème de Sylow on déduit qu'il n'y a qu'un seul 7-Sylow dans $N : P = \langle p\rangle$.

Par le théorème de Cauchy, il existe $n \in N$ d'ordre 3. Si il y a un seul 3-Sylow alors $pnp^{-1} \in \{e, n, ^2\}$. Mais comme n est d'ordre 3, il n'y a que deux cas possible :

(i) Si $np = pn$, alors $N = \langle np\rangle$ car $ppcm(3, 7) = 21$. Ce qui est absurde sachant que N n'est pas cyclique. (ii) Si $pn = n^2p$, on sait déjà que le 7-Sylow P est distingué dans N par définition de N. Donc il existe $k \in \{2, 3, 4, 5, 6\}$ tel que $n^{-1}pn = p^k$. Donc $np^k = pn = n^2p$ ce qui implique $np = p^k$ soir $n = p^{k-1}$. Donc $pn = np$ et on revient au cas précédent. Donc il y a 7 3-Sylows dans N. Mais sachant que pour $P \neq Q$, $|N_G(P) \cap N_G(Q)| = 3$, les 3-Sylows ne sont pas tous les mêmes si on les prend dans les normalisateurs de deux 7-Sylows différents. Donc il y a strictement plus de 7 3-Sylows dans G, soit par élimination, il y en a exactement 28.

Soit maintenant $H = N_G(M)$ ou $M = N_G(P) \cap N_G(Q)$, un 3-Sylow, On a d'après ce qui précède,

$$28 = N_3 = \frac{|G|}{|H|} = \frac{168}{|H|} \Longleftrightarrow |H| = \frac{168}{28} = 6.$$

Montrons que H n'est pas cyclique. En effet, supposons un instant que H soit cyclique. Si un groupe est cylique d'ordre 6, alors il contient au moins un élément d'ordre 6, notons le α. Il en contient en fait deux si l'on considère α^{-1}. Nous avons fixé P et Q pour trouver H, et donc si l'on considère l'ensemble des paires de 7-Sylows, de cardinal 28, on trouverait alors 28 groupes cycliques d'ordre 6, soit donc $28 \times 2 = 56$ élements d'ordre 6 dans le groupe G. Or on sait déjà que le nombre de 3-Sylows dans G est 28, et ils contiennent chacun deux éléments. Et enfin le nombre de 7-Sylows est 8 ce qui fait donc 48 éléments d'ordre 7. Avec tout ce monde, il ne reste plus beaucoup de place pour les 2-Sylows dont le cardinal est

8 d'après le théorème de Sylows.En effet dans cette configuration il n'y aurait qu'un seul 2-Sylows et il serait donc dinstingué dans G. Mais ceci est impossible comme G est simple. Tout cela rend donc le caracère cyclique de H absurde. Donc H n'est pas cyclique.

Recherche d'action non triviale dans G : Notons π un générateur de P l'un des 7-Sylows, et considérons l'application :

$$\begin{array}{rccc} \theta: & \mathbb{F}_7 & \longrightarrow & S\backslash\{P\} \\ & i & \longmapsto & \overline{\pi}(Q) = \pi^i Q \pi^{-i} \end{array} .$$

Cette application est bijective, en effet nous avons déja vu que P agit transitivement sur $S\backslash\{P\}$. Comme π engendre P, θ décrit cette action de P et on en déduit la surjectivité. Puis la bijectivité vient par cardinalité. De plus si l'on pose $\theta(\infty) = P$, on a alors θ qui forme une bijection de $\mathbb{P}^1(\mathbb{F}_7)$ sur S.

On identifiera alors dans la suite S et $\mathbb{P}^1(\mathbb{F}_7)$ au moyen de cette bijection. On remarque alors, avec la numérotation des points de S précédente, que $\overline{\pi}$ est une homographie de $\mathbb{P}^1(\mathbb{F}_7)$. En effet,

$$\overline{\pi}(i) = \overline{\pi}(\overline{\pi}^i(Q)) = \overline{\pi}^{i+1}(Q) = i+1. \text{ Donc } \overline{\pi}: \begin{array}{ccc} \mathbb{P}^1(\mathbb{F}_7) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_7) \\ z & \longmapsto & z+1 \end{array}$$

.

Essayons maintenant de trouver un autre élément de G dont l'action sur les 7-Sylows admet des propriétés remarquables. Posons alors μ un élément de M qui ne fixe pas tous les 7-Sylows. Alors comme μ n'est pas d'ordre 1, il est d'ordre trois. Supposons de plus l'existence de $k \in \mathbb{Z}$ tel que $\mu\pi\mu^{-1} = \pi^k$. Comme μ est d'ordre 3. $\pi = \mu^3\pi\mu^{-3} = \pi^{k^3}$. Comme π est d'ordre 7, on a alors $k^3 \equiv 1(7)$. Après quelques calculs on trouve que les seuls $k \in \{0,1,2,3,4,5,6\}$ tel que $k^3 \equiv 1(7)$ sont 2 et 4. Quitte à remplacer μ par μ^2, supposons $k = 2$. On a alors $\mu\pi = \pi^2\mu$. Utilisons cette égalité pour déterminer l'action de $\overline{\mu}$. Premièrement, on a $\overline{\mu}(0) = 0$, car $\mu \in N_G(Q)$. Par ailleurs,

$$\overline{\mu}(1) = \overline{\mu\pi}(0) = \overline{\pi}^2\overline{\mu}(0) = 2.$$

En réitérant ce procédé 6 fois on trouve alors que

$$\forall z \in \mathbb{P}^1(\mathbb{F}_7), \overline{\mu}(z) = 2z.$$

Par un calcul direct on montre alors que μ agit sur S en fixant P et Q. De plus il admet deux cycles d'ordre 3 sur $S\backslash\{P,Q\}$.

Cherchons un dernier élément de G d'action non triviale sur S pour pouvoir générer le groupe G.

Considérons le groupe quotient H/M de cardinal 2. Par le théorème de Cauchy on a alors l'éxistence d'un élément $\tau \in H/M$ d'ordre 2. On a déjà vu que $H = N_G(M)$ n'est pas cyclique et est d'ordre 6. De plus on sait également que μ est d'ordre 3 donc $\tau\mu\tau^{-1}$ l'est également mais cet élément est différent de μ. En effet si $\tau\mu\tau^{-1} = \mu$ alors H serait cyclique car généré par $\tau\mu$, or on a déjà vu que ce n'est pas le cas. On a alors $\tau\mu\tau^{-1} = \mu^{-1} = \mu^2 \iff \tau\mu = \mu^2\tau$. D'autre part, $\tau \notin M = N_G(P) \cap N_G(Q)$ et comme τ est d'ordre 2 alors par le théorème de Lagrange $\tau \notin N_G(P) \cup N_G(Q)$ qui est un groupe d'ordre impair. Donc $\overline{\tau}(P) \neq P$ et $\overline{\tau}(Q) \neq Q$. Cependant

$$N_G(\tau P\tau^{-1}) \cap N_G(\tau Q\tau^{-1}) = \tau\big(N_G(P) \cap N_G(Q)\big)\tau^{-1} = N_G(P) \cap N_G(Q) \text{ d'après l'égalité } \tau\mu\tau^{-1} = \mu^2.$$

Avec $\tau Q\tau^{-1}$ et $\tau P\tau^{-1}$ deux 7-Sylows vu que les Sylows sont stables par conjugaison. Or on a déjà vu en calculant l'action de μ que ce dernier ne fixait que P et Q. Donc si $R \in S\backslash\{P,Q\}$ on a $M \subset N_G(P) \cap N_G(Q) \cap N_G(R) = \{e\}$. Comme M est non-trivial, on a alors $\tau Q\tau^{-1} \in \{P,Q\}$ et $\tau P\tau^{-1} \in \{P,Q\}$. Par $(*)$ on en déduit que $\tau P\tau^{-1} = Q$ et $\tau Q\tau^{-1} = P$. On trouve alors enfin que $\tau(0) = \infty$ et $\tau(\infty) = 0$. Posons alors $a = \tau(1)$. Comme

$$\tau(2) = \tau\mu(1) = \mu^2\tau(1) = 4a \text{ alors } \tau(2) = 4a.$$

On calcule de même $\tau(4) = 2a$.

On remarque également que

$$\overline{\tau}(6) = \overline{\tau\mu}(3) = \overline{\mu}^2\overline{\tau}(3) = 4 \times \overline{\tau}(3) \text{ et par la même méthode on obtient } \overline{\tau}(3) = 4 \times \overline{\tau}(5); \overline{\tau}(5) = 2\overline{\tau}(6).$$

On retrouve les deux orbites de cardinal 3 sous l'action de $\langle\mu\rangle$: $\{\overline{\tau}(3), \overline{\tau}(5), \overline{\tau}(6)\}$ et $\{\overline{\tau}(1), \overline{\tau}(2), \overline{\tau}(4)\}$. Or $\tau\mu\tau^{-1} = \mu^{-1}$, donc $\mu\tau\mu^{-1} \neq \tau$, il y a alors trois involutions de H qui sont τ, $\mu\tau\mu^{-1}$ et $\mu^2\tau\mu^{-2}$. Donc quitte à remplacer τ par $\mu\tau\mu^{-1}$ ou $\mu^2\tau\mu^{-2}$, on peut choisir $\overline{\tau}(1)$ dans son orbite. On peut alors utiliser le :

Lemme 7. *τ ne fixe aucun point de S, ie $\forall k \in \mathbb{P}^1(F_7), \overline{\tau}(k) \neq k$*

Démonstration. En effet si l'on supposait l'existence de P fixe par τ cela signifierait qu'une involution fixe un point des 7-Sylows, mais on sait que le normalisateur de ce point est d'ordre 21 qui est impair, ce qui est absurde par le théorème de Lagrange. □

Cela nous permet de déduire que l'orbite de $\overline{\tau}(1)$ ne peut contenir 1. Donc $\overline{\tau}(1) \in \{3, 5, 6\}$. En prenant alors arbitrairement $a = 6$, on trouve après quelques calculs que $\forall k \in \mathbb{P}^1(F_7), \overline{\tau}(k) = \frac{-1}{k}$.

Générateur de $PSL_2(\mathbb{F}_7)$ et isomorphisme :

Proposition 4. $PSL_2(\mathbb{F}_7) = \langle\overline{\pi}, \overline{\mu}, \overline{\tau}\rangle$

Ce résultat est connus et la démonstration plutôt calculatoire, donc apporte peu à ce mémoire. Nous nous autoriserons donc à l'admettre. [8]

Donc $\varphi(G)$ contient $PSL_2(\mathbb{F}_7)$, et comme $|G| = |\varphi(G)| = |PSL_2(\mathbb{F}_7)|$, on en déduit que $\varphi(G) = PSL_2(\mathbb{F}_7)$. Enfin par injectivité de φ on a bien $G \simeq PSL_2(\mathbb{F}_7)$, ce qui est bien le résultat attendu.

2.2.2 Démonstration à l'aide du birapport

Création de l'ensemble de blocs par caractère équianharmonique : Comme nous sommes dans $\mathbb{F}_7$ et que 3 divise $7 - 1$ alors il existe trois racines cubiques de 1 : 1, 2, et 4. On pose alors $j = 2$.

Rappelons qu'un quadruplet $\{a, b, c, d\}$ d'éléments de $\mathbb{P}^1(\mathbb{F}_7)$ est dit équianharmonique si le birapport $[a, b, c, d]$ est dans $\{-j, -j^2\}$.

Remarque. (i) Dans le même ordre d'idée que lorsque qu'un quadruplet d'éléments de $\mathbb{P}^1(\mathbb{F}_7)$, si l'un des points est l'infini alors cela sinifie que l'un des trois autres est placé au milieu des deux restants, si un des points d'un quadruplet equianharmonique est placé à l'infini alors les trois autres forment un triangle équilatéral.
(ii) Rappelons nous que $j^2 + j + 1 = 0$ donc au vu des formules que nous avons évoquées, dans la partie sur 5, sur les valeurs possibles du birapport suite à une permutation des éléments du quadruplet, on se rend facilement compte qu'en permutant les points d'un quadruplet équianharmonique on ne peut obtenir que deux valeurs du birapport : $-j$ et $-j^2$.

Lemme 8. *Il existe* 28 *quadruplets équianharmoniques distincts dans $\mathbb{P}^1(\mathbb{F}_7)$*

Démonstration. Rappelons-nous que si l'on fixe trois point $\{a, b, c\}$ et une valeur λ dans $\mathbb{P}^1(\mathbb{F}_7)$, alors il existe un unique d distinct de a, b, et c, tel que $[a, b, c, d] = \lambda$. Multiplions alors le nombre de triplets ordonnés d'éléments distincts a, b, c $(8 \times 7 \times 6)$ par le nombre de valeurs possibles pour le birapport (il y en a deux : $-j$ et $-j^2$) que l'on divise par le nombre de permutations qui donne le même quadruplet :

$$\frac{8 \times 7 \times 6 \times 2}{4!} = 28.$$

Il y a donc bien 28 quadruplets équianharmoniques dans $\mathbb{P}^1(\mathbb{F}_7)$. □

Action de $\mathrm{PGL}_2(\mathbb{F}_7)$ et de $\mathrm{PSL}_2(\mathbb{F}_7)$ sur les blocs : Par préservation du birapport par homographie, $\mathrm{PGL}_2(\mathbb{F}_7)$ agit sur les quadruplets équianharmoniques. Demandons-nous alors quelles sont les propriétés remarquables de l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$ sur ces quadruplets.

Lemme 9. *L'ensemble des quadruplets équianharmoniques forment une unique orbite sous l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ et deux sous celle de $PSL_2(\mathbb{F}_7)$.*

8. Une démonstration est toute fois proposée en annexe.

Démonstration. La première partie se montre relativement simplement. Soit $Q = \{a, b, c, d\}$ un quadruplet équianharmonique, et soit $h \in \mathrm{PGL}_2(\mathbb{F}_7)$ l'homographie qui envoie (a, b, c) sur $(0, 1, \infty)$. Alors $h(d) = [\infty, 0, 1, h(d)] = [a, b, c, d]$. Comme Q est équianharmonique et que la valeur du birapport est invariante par homographie de $\mathrm{PSL}_2(\mathbb{F}_7)$, h envoie Q sur $\{\infty, 0, 1, 3\}$ ou $\{\infty, 0, 1, 5\}$. Enfin $s : z \mapsto 1 - z$ permute ces deux quadruplets,h ou sh envoie Q sur $\{\infty, 0, 1, 3\}$.

Passons à la deuxième partie. On calcule le cardinal de $\mathrm{PGL}_2(\mathbb{F}_7)$, en utilisant le fait que $GL_2(\mathbb{F}_7)$ est le nombre de base de $\mathbb{F}_7^2$. Donc l'ordre de $\mathrm{PGL}_2(\mathbb{F}_7) = \mathrm{GL}_2(\mathbb{F}_7)/\mathbb{F}_7^* I_2$ est 336. De même, par définition de $\mathrm{SL}_2(\mathbb{F}_7)$, son ordre est :

$$\frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{|\mathbb{F}_7^*|} = 336.$$

De plus, il n'y a que deux matrices scalaires dans $\mathrm{SL}_2(\mathbb{F}_7)$, ce sont : $\pm I_2$. Donc $\mathrm{PSL}_2(\mathbb{F}_7)$ est d'ordre $336/2 = 168$. On sait que $\mathrm{PGL}_2(\mathbb{F}_7)$ agit transitivement sur les 28 quadruplets équianharmoniques. Le stabilisateur de $Q_3 = \{0, 1, 3, \infty\}$ dans $\mathrm{PGL}_2(\mathbb{F}_7)$, $\mathfrak{A}$ est de cardinal $336/28 = 12$. Le groupe $\mathfrak{A}$ agit sur les éléments de Q_3 car on sait que si une homographie fixe trois points, c'est l'identité. Enfin comme $\mathfrak{A}$ est d'ordre 12, alors il est isomorphe à $\mathfrak{A}_4$,le seul sous-groupe d'indice 2 de $\mathfrak{S}_4 \simeq \mathfrak{S}_{Q_3}$. De ce fait regardons les homographies qui agissent sur Q_3 comme une double transposition. Il y a donc d'une part les homographies suivantes dans $\mathrm{PSL}_2(\mathbb{F}_7) \cap \mathfrak{A}$:

$$(\infty 0)(13) \leftrightarrow z \mapsto \frac{3}{z} \ ; \ (\infty 1)(03) \leftrightarrow z \mapsto \frac{z-3}{z-1} \ ; \ (\infty 3)(01) \leftrightarrow z \mapsto \frac{3z-3}{z-3}.$$

Modulo quelques calculs, on montre relativement facilement que ces homographies sont des involutions et qu'elles commutent sur trois points de Q_3 et donc sur $\mathbb{P}^1(\mathbb{F}_7)$ tout entier. De plus les déterminants des matrices correspondantes sont carrés donc les homographies exhibées sont des éléments de $\mathrm{PSL}_2(\mathbb{F}_7)$. Donc $\mathrm{PSL}_2(\mathbb{F}_7) \cap \mathfrak{A}$ contient un sous-groupe d'ordre 4. D'autre part il contient aussi l'élement d'ordre trois $g : z \mapsto \frac{1}{1-z}$ qui permute $\{\infty, 0, 1\}$ cycliquement et fixe 3. Donc $\mathfrak{A} \subset \mathrm{PSL}_2(\mathbb{F}_7)$ est le stabilisateur de Q_3 dans $\mathrm{PSL}_2(\mathbb{F}_7)$. Ainsi l'orbite de Q_3 a pour cardinal $168/12 = 14$. Comme $Q_5 = \{\infty, 1, 0, 5\}$ est dans la même orbite sous $\mathrm{PGL}_2(\mathbb{F}_7)$ que Q_3, son stabilisateur est conjugué à $\mathfrak{A}$ et donc de même cardinal : 14. □.

Cette partition étant faite, montrons maintenant que le passage au complémentaire des quadruplets dans $\mathbb{P}^1(\mathbb{F}_7)$ conserve cette structure particuliaire.

Lemme 10. *Le complémentaire d'un quadruplet équianharmonique dans $\mathbb{P}^1(\mathbb{F}_7)$ est équianharmonique. De plus, les deux quadruplets ainsi obtenus sont dans la même orbite sous l'action de $\mathrm{PSL}_2(\mathbb{F}_7)$.*

Démonstration. Commençons par montrer que le resultat est vrai pour $[\infty, 0, 1, 3] = 3 = [4, 2, 5, 6]$. L'homographie $h \in \mathrm{PSL}_2(\mathbb{F}_7)$ définie par $h(z) = (6z+2)/(4z+5)$ envoie $(4, 2, 5, 6)$ sur $(\infty, 0, 1, 3)$. Ce qui prouve le résultat pour $\{\infty, 0, 1, 3\}$. Soit maintenant $Q = \{a, b, c, d\}$ un quadruplet équianharmonique. D'après le lemme précédent, il existe $g \in \mathrm{PGL}_2(\mathbb{F}_7)$ tel que $g(Q) = \{\infty, 1, 0, 3\}$. On a alors, comme g est une bijection, le complémentaire de Q est envoyé par g sur $\{2, 4, 5, 6\}$, qui est équianharmonique. Enfin $g^{-1}hg$ envoie le complementaire de Q sur Q. Cela prouve le résultat dans le cas général. □

Corollaire 1. *Il y a exactement 14 triangles équilatéraux dans $\mathbb{F}_7$. Ce sont :*

013	124	235	346	450	561	602
015	126	230	341	452	563	604

Démonstration. D'après le lemme 4, on peut organiser les 28 quadruplets équiharmoniques en 14 paires complémentaires. Dans une paire donné, il y a exactement un quadruplet qui contient ∞. On en déduit alors que l'ajout ou le retrait de ∞ dans le bon quadruplet de chaques paires donne une bijection entre les triangles équilatéraux et les paires de quadruplets équianharmoniques.□

Action de $\mathrm{PGL}_2(\mathbb{F}_7)$ et de $\mathrm{PSL}_2(\mathbb{F}_7)$ sur les triangles : On peut commencer par remarquer la proposition suivante.

Proposition 5. *Il y a une action canonique de $\mathrm{PGL}_2(\mathbb{F}_7)$ sur les triangles équiatéraux. Ils appartiennent tous à la même orbite sous l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$, mais il y en a deux sous l'action de $\mathrm{PSL}_2(\mathbb{F}_7)$*

Démonstration. Au vu de la partition créée dans le corrolaire précédent, et comme il y a une unique orbite sous l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ sur les quadruplets équianharmoniques, $\mathrm{PGL}_2(\mathbb{F}_7)$ envoie un triangle équilatéral sur un autre, car son action commute avec la prise du complémentaire dans $\mathbb{P}^1(\mathbb{F}_7)$ (En effet faute de place, il n'y a que 8 ponts dans $\mathbb{P}^1(\mathbb{F}_7)$). On en déduit alors l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ sur l'ensemble des paires complémentaires de quadruplets équianharmoniques. Comme il y a une bijection entre les paires et les triangles équilatéraux, on hérite alors d'une action de $\mathrm{PGL}_2(\mathbb{F}_7)$ sur les triangles équilatéraux. En effet supposons abc un triangle équilatéral de $\mathbb{P}^1(\mathbb{F}_7)$, et $g \in \mathrm{PGL}_2(\mathbb{F}_7)$, il suffit de définir $g \cdot abc$ comme le triangle correspondant à la paire de quadruplets $g \cdot \{\{\infty, a, b, c\}; \mathbb{P}^1(\mathbb{F}_7) \backslash \{\infty, a, b, c\}\}$ D'où la première partie de la proposition.

Supposons maintenant deux triangles équilatéraux abc et $a'b'c'$, dans la même orbite sous $\mathrm{PSL}_2(\mathbb{F}_7)$. D'après le lemme 9, l'homographie qui envoie abc sur $a'b'c'$, envoie de la même façon $\{\{\infty, a, b, c\}, \mathbb{P}^1(\mathbb{F}_7) \backslash \{\infty, a, b, c\}\}$ sur $\{\{\infty, a', b', c'\}, \mathbb{P}^1(\mathbb{F}_7) \backslash \{\infty, a', b', c'\}\}$. Comme le lemme 10 implique que les paires de la forme $\{Q, \mathbb{P}^1(\mathbb{F}_7) \backslash Q\}$, où Q parcoure une orbite de $\mathrm{PSL}_2(\mathbb{F}_7)$, forme également une orbite de paire. On en déduit, par le lemme 9, qu'il y a deux orbites de paires sous $\mathrm{PSL}_2(\mathbb{F}_7)$, elles corespondent aux orbites des triangles. Dans le corollaire 1 les deux lignes sont exactement les deux orbites. □

Au vu de l'action de $\mathrm{PGL}_2(\mathbb{F}_7)$ et de $\mathrm{PSL}_2(\mathbb{F}_7)$ sur les triangles équilatéraux de $\mathbb{F}_7$ maintenant exhibée, tachons de structurer cet ensemble de points pour retrouver notre isomorphisme exceptionnel : $PSL_2(\mathbb{F}_7) \simeq GL_3(\mathbb{F}_2)$.

Pour cela commençons par définir une relation d'adjacence entre les triangles équilatéraux. On dit que deux triangles équilatéraux de $\mathbb{F}_7$ sont adjacents si ils ont deux sommets en communs. Il n'est pas difficle de vérifier (à la main) que tous les triangles du corollaire 1 sont adjacents à exactement trois triangles et ces trois triangles sont dans l'autre ligne. Considérons le graphe à quatorze sommets nommés par les triangles équilatéraux sur $\mathbb{F}_7$ dans lequel deux sommets sont reliés s'ils correspondent à deux triangles adjacents. On retrouve alors le graphe de Heawood. [9]

Si on distingue deux parties dans ce graphe, les triangles appartenant à la première et deuxième ligne du Corollaire 1, on retrouve alors le plan de Fano, où l'une des lignes forme l'ensemble des droites tandis que la deuxième forme celui des points. [10]

Isomorphisme entre $\mathrm{PSL}_2(\mathbb{F}_7)$ et $\mathrm{GL}_3(\mathbb{F}_2)$: Utilisons cette structure des triangles équilatéraux pour prouver le :

Théorème 6. *Le groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ est isomorphe au groupe $\mathrm{GL}_3(\mathbb{F}_2)$.*

Démonstration. Commençons par rappeler que le plan de Fano, que nous noterons dorénavant $\mathscr{P}$, peut être décrit comme les droites vectorielles de $\mathbb{F}_2^3$. En effet nommons les sommets par les vecteurs non nuls de $\mathbb{F}_2^3$ de telle sorte que si v et v' sont sur une même ligne alors le troisième point est $v + v'$. Ainsi une permutation f des points du plan $\mathscr{P}$ conservant une telle propriété est additive donc linéaire (car $\mathbb{F}_2^* = \{1\}$) si l'on rajoute le fait que $f(0) = 0$, puisque nous somme dans $\mathbb{F}_2$.

Posons alors $\phi : \mathrm{GL}_3(\mathbb{F}_2) \longrightarrow \mathrm{Aut}(\mathscr{P}); g \longmapsto \phi(g)$ de telle sorte que $\phi(g)$ associe au point de coordonnées (a, b, c) le point de coordonnées $g \cdot (a, b, c)$. Donc $\mathrm{Aut}(\mathscr{P}) \subset \phi(\mathrm{GL}_3(\mathbb{F}_2))$.

De même si $f \in \mathrm{GL}_3(\mathbb{F}_2)$, f est un automorphisme de $\mathbb{F}_2^3$ alors c'est une bijection de $\mathbb{F}_2^3 \backslash \{(0, 0, 0)\}$ et $\phi(f)$ préserve la strucutre du plan. Donc $\phi(\mathrm{GL}_3(\mathbb{F}_2)) \subset \mathrm{Aut}(\mathscr{P})$.

Enfin comme d'après la proposition 1, et au vu de la construction du plan $\mathscr{P}$, les triangles équilatéraux des points de $\mathscr{P}$ sont tous dans l'une des orbites de l'action de $\mathrm{PSL}_2(\mathbb{F}_7)$ qui est, rappelons le, fidèle (une homographie est fixé par son action sur trois points). Donc $\mathrm{Aut}(P) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. Par transitivité de la relation d'équivalence : isomorphie, $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2)$. □

2.3 $\mathrm{PSL}_2(\mathbb{F}_{11})$ et groupe d'automorphisme du (11,5,2)biplan

Montrons alors que comme avec 5 et 7, $\mathrm{PSL}_2(\mathbb{F}_{11})$ agit sur 11 points. Nous montrerons au passage que $\mathfrak{A}_5$ s'injecte dans $\mathrm{PSL}_2(\mathbb{F}_{11})$. Ce résultat est non trivial et sa démonstration non élémentaire.

9. Le graphe est disponible en annexes.
10. De même ce graphe est disponible en annexes.

2.3.1 Le (11,5,2) biplan et son groupe d' automorphismes

Ensemble de 11 points Commençons par décrire notre ensemble de 11 points, le (11,5,2)Biplan. C'est un ensemble de 11 5-uplets qui sont formés d'éléments de $\mathbb{F}_{11}$. (Pour simplifier la lecture on notera $X = 10$ et *abcde* pour $\{a, b, c, d, e\}$.) [11]

C'est un exemple de (11,5,2) *design* symétrique. En effet on peut remarquer que c'est un arrangement de 11 éléments dans 11 blocs. Chaque bloc contient exactement 5 éléments et chaque éléments est contenu dans exactement 5 blocs. Enfin deux blocs ont toujours exactement deux éléments en commun. Nous noterons dorénavant $\mathscr{B}$ ce (11,5,2)Biplan.

Groupe d'automorphismes du biplan On cherche alors à identififer le groupe des permutations des 11 points de $\mathbb{F}_{11}$ qui permutent égalements les quintuplets du Biplan. Pour cela on commençera par calculer son cardinal.

Définissions alors les groupes G, H, K, et L comme suit :

$$G = \mathrm{Aut}(B) \ ; \ H = Stab_G(B_1) \ ; \ K = Stab_H(1) \ ; \ L = Stab_K(3).$$

On a alors :

$$|G| = |Stab_L(4)| \cdot |Orb_L(4)| \cdot |Orb_K(3)| \cdot |Orb_H(1) \cdot |Orb_G(B_1)|.$$

Montrons alors le :

Théorème 7. $|G| = 660$

Démonstration. Soit $\in Stab_L(4)$. En particulier fixe B_1. Montrons alors que σ n'est autre que l'identité. On remarque alors que σ fixe les paires $\{1, 4\}$, $\{1, 3\}$ et $\{3, 4\}$ qui ne sont contenus que dans les blocs $B_4 = 46781$, $B_X = X1237$, et $B_0 = 02348$.Il suit que σ fixe B_4, B_X et B_0, ainsi il fixe les sous-ensembles $\{6, 7, 8\}$, $\{X, 2, 7\}$, et $\{0, 2, 8\}$. Cela n'est possible que si σ fixe les élements 2, 7, et 8, et donc aussi 6, X, et 0 ainsi que B_3. D'où σ fixe 5, et comme il fixe B_1, il fixe également 9. On en conclu donc que est l'identité.

Considérons maintenant $\alpha \in L$, c'est-à-dire que α fixe 1 et 3. La méthode précédente montre que toute permutation qui fixe trois points distincts dans G n'est autre que l'identité. Donc $\alpha = Id$ ou α permute de manère cyclique les point 4, 5 et 9 de B_1.Donc $Orb_l(4) = \{4, 5, 9\}$, et $|Orb_l(4)| = 3$. On peut remarquer sans trop de difficultés que K contient les permutations Id, $\beta = (3\ 4)(5\ 9)(2\ 8)(6\ X)$, $\gamma = (3\ 5)(4\ 9)(2\ 8)(7\ 0)$ et $\beta \circ \gamma$. Il vien alors que $Orb_K(3) = \{3, 4, 5, 9\}$, donc que $|Orb_K(3)| = 4$. On remarque également que H contient les puissances de $\mu = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ X\ 8)$. Il vien donc que $Orb_H(1) = \{1, 3, 4, 5, 9\}$, donc que $|Orb_H(1)| = 5$. Pour finir, G contient toute les puissance de $\tau = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 8\ X)$. Or la puissance k-ème de τ envoie B_0 sur B_k, donc $|Orb_G(B_0)| = 11$.

Donc, $|G| = 1 \times 3 \times 4 \times 5 \times 11 = 660$. □

2.4 Construction du (11,5,2)biplan

Pour bien comprendre l'action de $\mathrm{PSL}_2(\mathbb{F}_{11})$) sur les points du biplan, il faut comprendre comment ce dernier est construit. Sa construction est proche de celle des synthèmes et des triangles équilatéraux car encore une fois on se servira du birrapot.

Les lemmes suivants sont relativement simples.

Lemme 11. *Si a,et b sont harmoniquement conjugué à c et d, des points de* $\mathbb{F}_{11}$*, alors :*

$$[a, b, c, d] = -1 \Longleftrightarrow (a + b)(c + d) = 2(ab + cd).$$

En particulier :

Lemme 12. *Les points* ∞*, b sont harmoniquement conjugué à c, et d si et seulement si* $c + d = 2b$.

11. Vous trouverez le tableau en annexe.

Rappelons également que, si l'on considère une paire π d'éléments de $\mathbb{P}^1(\mathbb{F}_{11})$, alors son complémentaire se partitionne en 5 paires toute harmoniquement conjuguées à π. On en déduit alors qu'il y a $\binom{12}{2} \times 5/2 = 165$ quadruplets formés de deux paires harmoniquement conjugués dans $\mathbb{P}^1(\mathbb{F}_{11})$.

L'ensemble des $\binom{12}{4} - 165 = 330$ quadruplets formé de deux paires de $\mathbb{P}^1(\mathbb{F}_{11})$ dont le birapport est dans $\{3, 4, 5, 7, 8, 9\}$ étant stable par homographie, nous ne nous en préoccuperons pas.

Si un quadruplet est formé de deux paires harmoniquement conjuguées, il existe deux partions en deux paires de ce quadruplet tel que les deux paires ne soient pas harmoniquement conjuguées. Rappellons nous que l'on dira alors que cette partition chevauche le quadruplet.

Nous allons nous servir de cette caratéristique d'un qudruplet pour créer deux groupes de onze blocs d'éléments de $\mathbb{P}^1(\mathbb{F}_{11})$.

On rappelle que $\mathrm{PGL}_2(\mathbb{F}_{11})$ est trois fois transitif et $\mathrm{PSL}_2(\mathbb{F}_{11})$ l'est deux fois. Nous allons nous servir de ce fait et de l'invariance du birapport par homographie de $\mathrm{PSL}_2(\mathbb{F}_{11})$ pour, à partir de deux partitions de $\mathbb{P}^1(\mathbb{F}_{11})$ en paires qui se chevauchent deux à deux, retrouver toutes les partitions de $\mathbb{P}^1(\mathbb{F}_{11})$ ayant une telle caractéristique. Cherchons alors toute les paires de $\mathbb{P}^1(\mathbb{F}_{11})$ qui chevauchent $(0, \infty)$. D'après le lemme 12, si 0,et d sont harmoniquement conjugué à ∞, et b, alors $d = 2b$, donc $(0, \infty)$ chevauche toute les paires :

$$(12), (24), (36), (48), (5X), (61), (73), (85), (97), (X9).$$

Il faut maintenant que toutes les paires se chevauchent deux à deux. Si $(a, 2a)$ et $(b, 2b)$ se chevauchent, il y a deux situations possibles :

(i) Soit a et b sont harmoniquement conjugué à $2a$, et $2b$. Ce qui équivaut à $a^2 - 3ab + b^2 = 0$.

(ii) Soit a, et $2b$ sont harmoniquement conjugué à $2a$, et b. Ce qui équivaut à $a^2 + 4ab + b^2 = 0$.

Donc $(a, 2a)$ et $(b, 2b)$ se chevauchent si et seulement si à $(a^2 - 3ab + b^2)(a^2 + 4ab + b^2) = \frac{a^5 - b^5}{a - b} = 0$, soit $\frac{a}{b}$ est un carré différent de 1. Nous en déduisons alors les deux partitions de $\mathbb{P}^1(\mathbb{F}_{11})$ en paires qui se chevauchent deux à deux :

$$u_0 : (0\infty)(12)(48)(5X)(97)(36) \text{ et } v_0 : (0\infty)(16)(37)(9X)(58)(42).$$

On remarque au passage que ces deux partitions sont liés par l'homographie de $\mathrm{PGL}_2(\mathbb{F}_{11}) : z \mapsto \frac{1}{z}$.

Comme il y a $\binom{12}{2} = 66$ paires qui chevauchent avec 10 autres, il y a au maximum, $\frac{66 \times 10}{6 \times 5} = 22$ partitions de $\mathbb{P}^1(\mathbb{F}_{11})$ en six paires qui chevauchent deux à deux. L'homographie de $PSL_2(\mathbb{F}_{11})$, $T : z \mapsto t + 1$ nous permet de retrouver deux groupes de 11 partitions, et donc l'ensemble des 22 partition de $\mathbb{P}^1(\mathbb{F}_{11})$ possible. L'une contient u_0 et ses éléments seront notés u_i et l'autres contient v_0 et ses éléments seront notés v_i avec $i \in \{0, 1, ..., X\}$. chacun des deux ensembles est stable par action de $PSL_2(\mathbb{F}_{11})$ et on passe de l'un à l'autre par action de $PGL_2(\mathbb{F}_{11}) \backslash PSL_2(\mathbb{F}_{11})$. Remarquons de plus qu'il y a en tout (22×6) paires dans les partitions, et qu'une paire peut être contenue dans au plus deux partitions. Donc chaque paire appartient à deux partions, l'une dans l'ensemble des u_i et l'autre dans celui des v_i. [12]

C'est cette dernière remarque qui nous permettra de retrouver le biplan. En effet, considéront que deux partions u_i et v_j sont liées si elles ont en commun une paire. On retrouve alors le biplan en remarquant que chaque bloc B_j est composé des opposés des nombres i tel que v_i et u_j ne sont pas liés.

2.5 Le gain de tout ceci

2.5.1 Groupe de symétries du biplan

Par cette construction du biplan, on a alors directement l'action de $PSL_2(\mathbb{F}_{11})$ sur les onze points de $\mathscr{B}$. En effet l'action de $PSL_2(\mathbb{F}_{11})$ sur les points de $\mathbb{P}^1(\mathbb{F}_{11})$ induit, d'une part une action sur l'ensemble des v_i soit les éléments de $\mathbb{F}_{11}$ qui composent les blocs du biplan, et d'autres parts, une actions sur l'ensemble des u_i soit sur les blocs du biplan. de plus cette action est transitive puisque la construction de $\mathscr{B}$ repose sur l'action de $\mathrm{PSL}_2(\mathbb{F}_{11})$. On en deduit alors le théorème suivant.

Théorème 8. *Le groupe de symétries de $\mathscr{B}$ est isomorphe à* $\mathrm{PSL}_2(\mathbb{F}_{11})$.

12. Je vous renvoie au tableau en annexes.

Démonstration. Dans le Théorème 7 nous avons montré que $\mathrm{PSL}_2(\mathbb{F}_{11})$ était un groupe de cardinal 660 qui agissant non trivialement et transitivement sur les points de $\mathscr{B}$ donc qui s'injectait dans le groupe de symétrie du biplan. On montre de même que le groupe agit fidèlement. En effet de même que nous avons procédé dans la démonstration du Théorème 7, on montre petit à petit que si un élément de $\mathrm{PSL}_2(\mathbb{F}_{11})$ fixe tous les blocs du biplan alors il fixe tous les u_i donc les v_i et par conséquent les points de $\mathbb{P}^1(\mathbb{F}_{11})$. Comme une homographie qui fixe trois points n'est autre que l'identité, c'est en particulier le cas quand elle en fixe onze. D'où la fidélité de l'action. Nous avions commencé la partie par calculer le cardinal du groupe de symétrie du Biplan, 660. Donc l'isomorphisme entre les deux groupes s'obtien par cardinalité. □.

Notons alors Θ l'isomorphisme de groupe de $\mathrm{PSL}_2(\mathbb{F}_{11})$ dans le groupe de symétries du (11,5,2)biplan.

Un gain inattendu Il exite un autre gain notable de cette acion de $\mathrm{PSL}_2(\mathbb{F}_{11})$ sur le biplan. En effet considéront le stabilisateur d'un point de ce dernier dans $\mathrm{PSL}_2(\mathbb{F}_{11})$. Par exemple $B_1 = \{1,3,4,5,9\}$ correspondant à u_0. En restreignant le groupe fixateur de u_0 à ce sous ensemble de cardinale 5 on obtient le morphisme de groupe :

$$\begin{array}{rccc} \Phi: & \mathrm{Stab}_{\Theta(\mathrm{PSL}_2(\mathbb{F}_{11}))}(B_2) & \longrightarrow & \mathfrak{S}_5 \simeq \mathfrak{S}_{\{1,3,4,5,9\}} \\ & \tau & \longmapsto & \tau_{|\{1,3,4,5,9\}} \end{array} .$$

Ce morphisime Φ est injectif, en effet si $\tau \in \Theta(\mathrm{PSL}_2(\mathbb{F}_{11}))$ fixe 5 points alors $\Theta^{-1}(\tau)$ aussi. Et donc $\Theta^{-1}(\tau)$ et τ sont l'identité. Donc $\Phi(\mathrm{Stab}_{\Theta(\mathrm{PSL}_2(\mathbb{F}_{11}))}(u_0))$ est un sous-groupe du groupe de symétrie du (11,5,2)Biplan agisant transitivement et d'odre 660. On en déduit alors que $|\mathrm{Stab}(B_1)| = \frac{660}{11} = 60 = \frac{5!}{2}$.

La proposition 1 nous permet alors de dire que $\mathrm{Stab}(u_0)$ est isomorphe à $\mathfrak{A}_5$, et donc que $\mathfrak{A}_5$ s'injecte non trivialement dans $\mathrm{PSL}_2(\mathbb{F}_{11})$. Ce résultat étant non-trivial et les démontration abituelle peu-élémentaire, en déduire une telle démonstration est un gain non négligeable.

3 Uniformisation et création du système de Steiner

3.1 Reformulation uniforme des actions de $\mathrm{PSL}_2(\mathbb{F}_p)$

D'après tout ce qui précède on peut dire que pour $p = 5, 7, 11$ on a trouvé géométriquement un ensemble de p partitions de $\mathbb{P}^1(\mathbb{F}_p)$ en $\frac{p+1}{2}$ paire que nous associrons à des transpositions stables par action de $\varphi(\mathrm{PSL}_2(\mathbb{F}_p))$, où $\varphi : \mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_p)} \simeq \mathfrak{S}_{p+1}$.

Dans un premier temps avec $\mathbb{F}_5$: En effet, si l'on note 6 l'infini et 5 le zéro de $\mathbb{P}^1(\mathbb{F}_5)$ alors à chaque chaque paire harmoniquement séparée on peut associer une transposition de $\mathfrak{S}_6$ de tel sorte que l'on ai 5 triples transpositions. Par exemple $\big\{\{\infty, 0\}, \{1,4\}, \{2,3\}\big\}$ donne la triple-transpositon (06)(14)(23). Faisons agir $\mathrm{PSL}_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$ que l'on identifie à $\{1,2,3,4,5,6\}$. Par invariance du birapport par action de $\mathrm{PSL}_2(\mathbb{F}_5)$ on en déduit alors que l'ensemble des 5 triples transpositions est stable par conjugaison avec $\varphi(\mathrm{PSL}_2(\mathbb{F}_5))$.

Puis avec $\mathbb{F}_7$: De même si l'on considère les triangles équilatéraux de $\mathbb{F}_7$. Prenons-en un abc dans l'orbite sous $\mathrm{PSL}_2(\mathbb{F}_7)$ de 013. Considérons alors le quadruplet $\{\infty, a, b, c\}$ et sont complémentaire dans $\mathbb{P}^1(\mathbb{F}_7)$, $\{d, e, f, g\}$. On a vu que, quitte à réordonner, $[\infty, a, b, c] = 3 = [d, e, f, g]$. Considérons alors l'ensemble des quadruples transpositions de la frome $(a\infty)(bc)(de)(fg)$, où abc parcourt l'orbite de 013 sous l'action de $\mathrm{PSL}_2(\mathbb{F}_7)$, où de nouveau, on associe à 0 la valeur 7 et à ∞ la valeur 8. On retrouve alors un ensemble de 7 quadruples transpositions de $\mathfrak{S}_8$ stables par conjugaison avec $\varphi(\mathrm{PSL}_2(\mathbb{F}_7))$ pour les même raisons qu'avec $\mathbb{F}_5$.

Le résultat aurait été le même si on c'était placé dans l'orbite de 015.

Enfin avec $\mathbb{F}_{11}$: Si l'on reprend les même notations que dans la partie portant sur la construction du biplan on l'ensemble des hexades u_i qui est stable par action de $\mathrm{PSL}_2(\mathbb{F}_{11})$. Encore une fois associons $\mathbb{P}^1(\mathbb{F}_{11})$ à $\{1, 2, ..., 11, 12\}$. Posons pour i allant de 1 à 11, $\tau_i \in \mathfrak{S}_{12}$ le produit des 6 transpositions qui permutent les paires de u_i. Alors comme l'ensemble des u_i est par construction stable par action $\mathrm{PSL}_2(\mathbb{F}_{11})$, on en déduit que l'ensemble des τ_i est stable par conjugaison avec $\varphi(\mathrm{PSL}_2(\mathbb{F}_{11}))$.

En fait même avec $\mathbb{F}_3$ Comme il n'y a que peu de quadruplets possibles dans $\mathbb{P}^1(\mathbb{F}_3)$: il n'y en a que trois. Toujours par invariance du birraport par actions de $\mathrm{PSL}_2(\mathbb{F}_3)$, les doubles transpositions $(\infty 0)(12)$ et $(\infty 1)(02)$ sont stables par conjuguaison avec $\varphi(\mathrm{PSL}_2(\mathbb{F}_3))$

On en déduit alors une méthode homogène pour d'écrire l'action de $\mathrm{PSL}_2(\mathbb{F}_p)$ agit sur p points pour $p = 3, 5, 7, 11$.

3.2 Une construction de S(5,6,12)

D'après ce que nous avons vu sur 11, nous pouvons penser qu'il est possible de retrouver un S(5,6,12) système de steiner ou les 12 points seraient $\mathbb{F}_{11} \cup \{\infty\}$ en faisant agir $\mathrm{PSL}_2(\mathbb{F}_{11})$ sur l'hexade, notée S_0, $\{\infty, 1, 3, 4, 5, 9\}$. On veut montrer que l'orbite $\mathscr{S}$ de S_0 sous le groupe $\mathrm{PSL}_2(\mathbb{F}_{11})$ est un système de Steiner $S(5, 6, 12)$.

Pentades

Lemme 13. *Il y a deux orbites de pentades sous* $\mathrm{PSL}_2(\mathbb{F}_{11})$ *:*
- *celle de* $\{1, 3, 4, 5, 9\}$*, qui est de cardinal* 132 *;*
- *celle de* $\{\infty, 1, 3, 4, 9\}$*, qui est de cardinal* 660*.*

On peut les distinguer de la façon suivante :
- *une pentade est dans l'orbite de cardinal* 132 *SSI elle ne contient aucune division harmonique ;*
- *une pentade est dans l'orbite de cardinal* 660 *SSI sur les* 5 *quadruplets qu'elle contient,* 2 *sont harmoniques et* 3 *ne le sont pas.*

Démonstration. Soit P une pentade. Montrons que son stabilisateur H est d'ordre 1 ou 5. Comme une homographie est définie par l'image de 3 points, la restriction à P définit une injection de H dans $\mathfrak{S}_5$, de cardinal 120. Il suffit donc de montre que H ne contient pas d'élément d'ordre 2 ou 3.

Soit h un élément de H supposé d'ordre 2 ou 3. Comme ni $|P|(= 5)$, ni $\left|\mathbb{P}^1(\mathbb{F}_{11})\right| - |P|(= 7)$ ne sont divisible par 2 ou 3, il y a au moins deux points fixés par h, un dans P et un dans son complémentaire. Quitte à conjuguer h parun élément $g \in \mathrm{PSL}_2(\mathbb{F}_{11})$ et à remplacer P par $g(P)$, on peut supposer que h fixe ∞ et 0. Cela signifie que h est de la forme $z \mapsto az$, où a est un carré de $\mathbb{F}_{11}$ qui a le même ordre que h. Comme ni 2 ni 3 ne divisent l'ordre du groupe des carrés $\mathbb{F}_{11}^{\times 2}$, cela entraîne que h ne peut être d'ordre 2 ou 3.

Supposons que h soit d'ordre 5 dans $\mathrm{PSL}_2(\mathbb{F}_{11})$. Comme 5 ne divise pas $12 = |\mathbb{P}^1(\mathbb{F}_{11})|$, l'élément h a nécessairement au moins deux points fixes. Comme ci-dessus, quitte à conjuguer h, on peut supposer que $h(0) = 0$ et $h(\infty) = \infty$, c'est-à-dire que h est de la forme $z \mapsto az$. Alors, les orbites de h sont $C = \{1, 3, 4, 5, 9\}$ et $-C = \{2, 6, 7, 8, X\}$, deux pentades stables.

Ainsi, soit P est dans l'orbite de C, auquel cas son stabilisateur est d'ordre 5 ; soit P n'est pas dans l'orbite de C, auquel cas son stabilisateur est trivial. L'orbite de C est d'ordre $660/5 = 132$ et il y a $\binom{12}{5} - 132 = 792 - 132 = 660$ pentades en plus qui forment donc une unique orbite, par invariance du birapport par homographie. Il suffit donc de calculer neuf birapports à partir de $\{1, 3, 4, 5, 9\}$ et $\{\infty, 1, 3, 4, 9\}$:

$$[3, 4, 5, 9] = 9, \quad [1, 4, 5, 9] = 8, \quad [1, 3, 5, 9] = 7, \quad [1, 3, 4, 5] = 7,$$
$$[1, 3, 4, 9] = 5, \quad \underline{[\infty, 3, 4, 9] = 6}, \quad \underline{[\infty, 1, 4, 9] = X}, \quad [\infty, 1, 3, 9] = 4, \quad [\infty, 1, 3, 4] = 7.$$

On voit bien par invariance du birraport que $\{1, 3, 4, 5, 9\}$ et $\{\infty, 1, 3, 4, 9\}$ sont dans des orbites différntes et par invariance du birraport par homogrpahie d'où le résultat.

Hexades

Lemme 14. *L'ensemble $\mathscr{S}$ contient* 132 *éléments (appelés* blocs *plus bas).*

Démonstration. Comme $132 = 660/5$, il suffit de montrer que le stabilisateur de B_0 est de cardinal 5. On a vu que c'est l'ordre du stabilisateur de $B_0 \setminus \{\infty\}$ donc il suffit de montrer que ces deux stabilisateurs coïncident. Parmi les $\binom{6}{4} = 15$ quadruplets de points de B_0. Le calcul des 6 derniers birapports [13] montre que le point ∞ fait partie de tous les quadruplets harmoniques contenus dans B_0 et que c'est le seul. On en déduit alors que le point ∞ est fixé par tout élément du stabilisateur de B_0. En effet, par invariance du birapport par homographie, $g(\infty)$ est l'unique point de $g(B_0)$ qui appartient aux quadruplets harmoniques inclus dans $g(B_0)$. Comme $g(B_0) = B_0$, on a : $g(\infty) = \infty$.

La proposition suivante exprime le fait que $\mathscr{S}$ est un système de Steiner $S(5, 6, 12)$.

Proposition 6. *Pour toute pentade P, il existe un unique bloc $B \in \mathscr{S}$ qui contient P.*

Démonstration. Notons $\mathscr{P}_5$ l'ensemble des pentades et $\mathscr{I} = \big\{(P, B) \in \mathscr{P}_5 \times \mathscr{S},\ P \subset B\big\}$.

On veut montrer que $p_1 : \mathscr{I} \to \mathscr{P}_5,\ (P, B) \mapsto P$ est bijective. Or un bloc $B \in \mathscr{P}$ contient $\binom{6}{5} = 6$ pentades, d'où l'égalité : $|\mathscr{I}| = 6 \times |\mathscr{S}| = 792 = |\mathscr{P}_5|$. Il suffit donc de montrer que p_1 est surjective.

Soit donc $P \in \mathscr{P}_5$. Si P est dans l'orbite de cardinal 132, c'est que $P = g \cdot \{1, 3, 4, 5, 9\}$ pour $g \in \mathrm{PSL}_2(\mathbb{F}_{11})$ convenable : dans ce cas, la pentade P est contenue dans le bloc $g(B_0) \in \mathscr{S}$. Si P est dans l'orbite de cardinal 660, c'est que $P = g \cdot \{\infty, 1, 3, 4, 9\}$ pour $g \in \mathrm{PSL}_2(\mathbb{F}_{11})$ convenable, donc P est contenue dans le bloc $g(B_0) \in \mathscr{S}$. Cela montre que pour toute pentade P, il existe un bloc $B \in \mathscr{S}$ tel que $(P, B) \in \mathscr{I}$: autrement dit, p_1 est surjective et c'est gagné.

Par l'action de $\mathrm{PSL}_2(\mathbb{F}_{11})$ sur une hexade de $\mathbb{P}^1(\mathbb{F}_{11})$ bien choisie on arrive donc à retrouver une construction non trivial et logique du $S(5, 6, 12)$. Ce qui était le resulat attendu.

Références

[1] Michel DEMAZURE. *Cours d'algèbre.* Cassini 2009

[2] Daniel PERRIN. *Cours d'algèbre.* Collection de l'Ecole Normale Supérieure de Jeunes Filles 1990

[3] Anne Cortella. *Algèbre Théorie des groupes* . Vuibert 2011

[4] Ezra BROWN. *The Fabulous (11, 5, 2) Biplane.*MATHEMATICS MAGAZINE VOL. 77, NO. 2, AVRIL 2004

[5] W.L. EDGE. *PGL(2,11) and PSL(2,11).* JOURNAL OF ALGEBRA 97,492-504 1985

[6] Ezra BROWN et Nicholas LOEHR. *Why is PSL(2, 7) ≅ GL(3, 2) ?.* Ed Scheinerman Octobre 2009

13. Voir en annexe.

Annexes

Annexe 1 : Démonstration de la proposition 1

Démonstration. Commençons par l'éxistence. En effet il en exite un car le noyaux de la signature vérifie les propriétés demandées.

Voyons ensuite l'uncité. On a dans un premier temps en toute généralité le lemme suivant.

Lemme 15. *Si H est d'indice 2 dans le grouep G, alors il est distingué.*

Démonstration. En effet, soit $g\backslash H$. On a d'une part, $gH \subset G\backslash H$ et d'autre parts $|gH| = |H| = |G| - |H|$. on a donc $gH = G\backslash H$. On montre de la même manière que $Hg = G\backslash H$. On a donc $gH = Hg$ soit, $gHg^{-1} = H$. □

Annexe 2 : démonstration du lemme 3

Démonstration. En effet la valeur du birapport des quatres points est dans l'ensemble $\mathbb{P}^1(\mathbb{F}_p)\backslash\{0; 1; \infty\}$, donc ici il sagit de $\{2; 3; 4\} = \{2; 1/2; -1\}$. Supposons alors $[z_1, z_2, z_3, z_4] = \frac{1}{2}$ alors $[z_2, z_1, z_3, z_4] = 2$ et $[z_2, z_1, z_3, z_4] + [z_2, z_3, z_1, z_4] = 1$ donc $[z_2, z_3, z_1, z_4] = -1$. Donc le conjugué harmonique de z_5 par z_1 et z_2 est z_6 puisque ça ne peut etre ni z_3, ni z_4, par existance et unicité du conjugué harmonique. Enfin le conjugué de z_5 ne peut être lui même au vu de la remarque précédente faite sur les points fixes de l'application Γ. De meme on montre que le conjugué harmonique de z_5, par z_3 et z_4 est z_6. □.

Annexe 3 : Démonstration alternative du lemme 5

Démonstration. La deuxième méthode est la suivante : On commence par constater que l'ordre de K divise 12 par le théorème de Lagrange. En effet en notant G_x le stabilisateur d'un point $x \in S$ par action de G on a K est un sous-groupe de G_x. Or $|G_x| = \frac{|G|}{|O_x|} = \frac{60}{5}$ où O_x est l'orbite de x par action de G. Supposons maintenant qu'il ne soit pas trivial, alors par les deux théorèmes de Sylow K contient au moins un sous-groupe d'ordre 2 et un sous-groupe d'ordre 3 ($12 = 4 \times 3$). Et donc K contient au moins un élément d'ordre 2 et un élément d'ordre 3 ainsi que tous les éléments de $PGL_2(\mathbb{F}_5)$ qui leur sont conjugués.

Examinons ces éléments. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_5)$ et $h_A : z \longmapsto \frac{az+b}{cz+d}$. On a évidement $h_A = Id \iff A = \lambda I_2$ avec $\lambda \in \mathbb{F}_5$. Suposons h_A^2 d'ordre 2, alors

$$\begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix} = A^2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \iff \begin{cases} a^2 + bc = d^2 + bd \\ b(a+d) = 0 \\ c(a+d) = 0 \end{cases}.$$

Montrons alors le :

Lemme 16. *h_A est d'ordre 2 $\iff tr(A) = 0$*

Démonstration. Le premier sens se montre relativement facilement à l'aide du théorème de Calay-Hamilton :

$$tr(A) = 0 \Longrightarrow \varkappa_A(A) = A^2 - tr(A)A + det(A)I_2 = A^2 + det(A)I_2 = 0 \Longrightarrow h_A^2 = h_{A^2} = Id$$

. Pour la réciproque, supposons $a + d \neq 0$. Alors $a - d = 0$ ie $a = d$ et $b = c = 0$. Donc $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ avec $a \neq 0$ sinon $a + b = 0$. Donc $h_A = Id$ et h_A est d'ordre 1. □

Donc $\varkappa_A = X^2 + det(A)$. On examine alors deux cas : (i) Si $-det(A)$ est résidus quadratique de $\mathbb{F}_5$ alors $\varkappa_A$ est scindé simple, donc A est diagonalisable, et $A \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \lambda$ avec $\lambda \in \mathbb{F}_5$. Donc $h_A(z) = -z$. (ii) Si $-det(A)$ n'est pas résidus quadratique, $\varkappa_A$ est irréductible, donc A n'admet pas de valeur propre dans $\mathbb{F}_5$. Donc soit $e_1 \in \mathbb{F}_5^2\backslash\{(0, 0)\}$. $B = (e_1, A \cdot e_1)$ est alors une famille libre donc une

base de $\mathbb{F}_5^2$, nous noterons B_0 sa base canonique. soit f un endomorphisme de $\mathbb{F}_5^2$ tel que $[f]_{B_0} = A$. Alors $[f]_B = \begin{pmatrix} 0 & -det(A) \\ 1 & 0 \end{pmatrix}$. Donc $A \begin{pmatrix} 0 & -det(A) \\ 1 & 0 \end{pmatrix}$.

Les seuls non-résidus quadratiques dans $\mathbb{F}_5$ sont 2 et -2. Il y a alors deux classes de conjugaisons d'éléments d'ordre 2 dans $GL_2(\mathbb{F}_5)$: celle de $A = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$ et celle de $A' = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Montrons alors que h_A et $h_{A'}$ sont conjuguées. Notons $B = 2A$ avec bien sûr $h_A = h_B$. On a B A' en faisant le changement de base $e_1' = e_1$ et $e_2' = 2e_2$. Donc h_A et $h_{A'}$ sont conjuguées.

On en deduit alors que tous les éléments d'ordre 2 sont conjugués à $h_1 : z \longmapsto -z$, ou $h_2 : z \longmapsto 2/z$. Qu'en est il des éléments d'ordre 3 ?

Si h_A est un élément d'ordre 3, $h_A^3 = Id$ soit $A^3 = \lambda I_2$ avec $\lambda \in \mathbb{F}_5*$. Comme 3 ne divise pas 4, alors pour tout élément α du groupe multiplicatif $\mathbb{F}_5^*$, $\alpha^3 \neq 1$, d'après le théorème de Lagrange. Donc le morphisme de groupe $c : \mathbb{F}_5^* \longrightarrow \mathbb{F}_5^*, x \longmapsto x^3$ est injectif et donc bijectif par cardinalité. Donc quitte à remplacer A par $A' = \frac{1}{c^{-1}(\lambda)}A$,on peut supposer $A^3 = I_2$. Si A admet un valeur propre dans $\mathbb{F}_5$, alors sont cube vaut 1, et par injectivité de $c$cette valeur propre est 1. L'autre valeur propre, μ, est aussi dans $\mathbb{F}_5$ puisque $\lambda + \mu = tr(A) \in \mathbb{F}_5$, et pour les même raison que λ, elle vaut aussi 1. Donc A est trigonalisable et on a :

$$A \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \text{ avec } b \in \mathbb{F}_5.$$

Le calcul du cube de A montre que $b = 0$ ce qui est absurde puisque l'dentité est d'ordre 1 et pas 3. Ainsi les valeurs propre de A sont les racines du polynôme caractéristique de $A : X^2 + X + 1$. Mais alors prenons un vecteur propre $e_1 \in \mathbb{F}_5^2$ non nul. Comme A n'as pas de valeur propre dans $\mathbb{F}_5$, la famille (e_1, Ae_1) est libre donc c'est une base de $\mathbb{F}_5$. Dans cette base, la matrice de l'aplication linéaire représenté par A dans la base canonique est : $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, au vu du polynome caractéristique.

Donc les seuls éléments d'ordre trois sont conjugués à $h_3 : z \longmapsto \frac{1}{1-z}$.

On remarque assez facilement que h_1,h_2 et h_3 exercent une action non triviale sur S donc aucun d'entre eux n'appartient à K, soit $3 \nmid |K|$ et $2 \nmid |K|$. Donc $|K| = 1$, soit $K = \{e\}$.□

Annexe 4 : Démonstration de la proposition 4

Démonstration. Considérons h l'homographie de $\mathrm{PSL}_2(\mathbb{F}_7)$ défini par $h(z) = \frac{az+b}{cz+d}$.

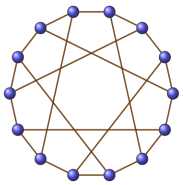
Si $c = 0$, on a alors $ad = 1$, soit $d = a^{-1}$, donc $h(z) = a^2 z + ab$. Les carrés non nul de $\mathbb{F}_7$ sont 1, 2 et 4, donc $h = \overline{\pi}^{ab} \cdot \overline{\mu}^j$ pour un j convenable dans $\{0, 1, 2\}$.

Sinon si $h(z) = \frac{az+b}{cz+d}$ avec $c \neq 0$. On a alors

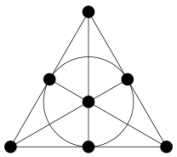
$$h(z) = (ac^{-1}) + \frac{bc - ad}{c(cz + d)} = (ac^{-1}) + \frac{-1}{c^2 z + cd}.$$

Donc si on pose $c^2 = 2^j$, il est alors imédiat que $h = \overline{\pi}^{ac^{-1}} \cdot \overline{\tau} \cdot \overline{\pi}^{cd} \cdot \overline{\mu}^j$. On a donc bien $PSL_2(\mathbb{F}_7) = \langle \overline{\pi}, \overline{\mu}, \overline{\tau} \rangle$. □

Annexe 5 : Le graphe de Heawood



Annexe 6 : Le plan de Fano



Annexe 7 : Le (11,5,2) biplan

$$B_1 = 13459 \quad B_2 = 2456X \quad B_3 = 35670 \quad B_4 = 46781 \quad B_5 = 57892 \quad B_6 = 689X3$$
$$B_7 = 79X04 \quad B_8 = 8X015 \quad B_9 = 90126 \quad B_X = X1237 \quad B_0 = 02348$$

Annexe 7 : Tableau des partitions en paires des onze points

u_0	$(0\infty)(12)(48)(5X)(97)(36)$	$(0\infty)(16)(37)(9X)(58)(42)$	v_0
u_1	$(1\infty)(23)(59)(60)(X8)(47)$	$(1\infty)(27)(48)(X0)(69)(53)$	v_0
u_2	$(2\infty)(34)(6X)(71)(09)(58)$	$(2\infty)(38)(59)(01)(7X)(64)$	v_0
u_3	$(3\infty)(45)(70)(82)(1X)(69)$	$(3\infty)(49)(6X)(12)(80)(75)$	v_0
u_4	$(4\infty)(56)(81)(93)(20)(7X)$	$(4\infty)(5X)(70)(23)(91)(86)$	v_0
u_5	$(5\infty)(67)(92)(X4)(31)(80)$	$(5\infty)(60)(81)(34)(X2)(97)$	v_0
u_6	$(6\infty)(78)(X3)(05)(42)(91)$	$(6\infty)(71)(92)(45)(03)(X8)$	v_0
u_7	$(7\infty)(89)(04)(16)(53)(X2)$	$(7\infty)(82)(X3)(56)(14)(09)$	v_0
u_8	$(8\infty)(9X)(15)(27)(64)(03)$	$(8\infty)(93)(04)(67)(25)(1X)$	v_0
u_9	$(9\infty)(X0)(26)(38)(75)(14)$	$(9\infty)(X4)(15)(78)(36)(20)$	v_0
u_X	$(X\infty)(01)(37)(49)(86)(25)$	$(X\infty)(05)(26)(89)(47)(31)$	v_0

Annexe 8 : Calcul des six birapports manquants les 6 derniers birapports sont :

$$\underline{[\infty,1,3,5]=2}, \quad [\infty,1,4,5]=5, \quad \underline{[\infty,1,5,9]=2}, \quad \underline{[\infty,3,4,5]=2}, \quad [\infty,3,5,9]=3, \quad [\infty,4,5,9]=5.$$