Tuteur : Odile Garotta

Le groupe simple à 168 éléments

Jean-Mathieu Magot

TER de l'année 2009

Table des matières

1 Existence d'un groupe simple de cardinal 168 **3**

2 Étude de la structure d'un groupe simple à 168 éléments **4**
2.1 Étude des 7-Sylow de G et des éléments d'ordre 7 5
2.2 Étude des 3-Sylow de G et des éléments d'ordre 3 5
2.3 Ordres des éléments de G 6
2.4 Étude des 2-Sylow et des éléments d'ordre 2, 4 et 8 6
2.5 Classes de conjugaison de G 8
2.6 Les sous-groupes de Klein de G 8

3 Unicité du groupe simple d'ordre 168 **9**
3.1 Action particulière de G 9
3.2 Théorème d'unicité 9

4 Les sous-groupes de G **12**
4.1 Zoologie des sous-groupes de G 12
4.2 Action par conjugaison de G sur ses sous-groupes 16

5 Les automorphismes de G **16**
5.1 Le sous-groupe des automorphismes intérieurs de G 16
5.2 Le groupe des automorphismes de G 18

6 La table des caractères de G **19**

7 Bibliographie **23**

Introduction

C'est un fait, il n'existe qu'un seul groupe simple à 168 éléments à isomorphisme près. Nous nous proposons ici dans un premier temps de démontrer ce résultat, ce qui requierra d'étudier un minimum ce que peut être la structure d'un tel groupe, puis, voyant ce groupe comme le groupe des automorphismes du plan projectif à 7 points, nous serons en mesure de prouver son unicité. Dans un second temps, nous compléterons la description de la structure du groupe simple d'ordre 168 par l'identification de tous ses sous-groupes, nous observerons aussi leurs intéractions et enfin déterminerons leur orbites sous l'action par conjugaison. Nous poursuivrons sur la détermination du groupe des automorphismes du groupe simple à 168 éléments, et, enfin, établirons sa table des caractères des représentations irréductibles complexes.

1 Existence d'un groupe simple de cardinal 168

Comme nous l'avons annoncé, nous allons commencer par étudier la structure d'un groupe simple à 168 éléments, mais auparavant, il convient de vérifier qu'un tel groupe existe. Observons le cas du groupe $G \triangleq PSL_3(\mathbb{F}_2)$.

Définitions : (i) Où $Z(SL_n(\mathbb{F}_q))$ est le centre de $SL_n(\mathbb{F}_q)$:

$$PSL_n(\mathbb{F}_q) \triangleq \frac{SL_n(\mathbb{F}_q)}{Z(SL_n(\mathbb{F}_q))}$$

(ii) On appelle plan projectif associé à un espace vectoriel E de dimension 3, l'ensemble de ses droites vectorielles, et on le note $\mathbb{P}(E)$. Si E est un $\mathbb{K}$-espace vectoriel de dimension 3, on note : $\mathbb{P}(E) = \mathbb{P}^2(\mathbb{K})$.

(iii) Où E est un espace vectoriel sur un corps $\mathbb{K}$ et n un entier :

$$PGL_n(E) \triangleq \frac{GL_n(E)}{Id_E.\mathbb{K}^\times}$$

Remarques : (i) On notera toujours le centre ainsi, on utilisera aussi cette notation pour parler du centralisateur (ou commutant) d'un élément.

(ii) Dans notre cas, $(n,q) = (3,2)$, on peut faire les identifications suivantes :

$$PSL_3(\mathbb{F}_2) = SL_3(\mathbb{F}_2) = GL_3(\mathbb{F}_2) = PGL_3(\mathbb{F}_2)$$

Il suffit de remarquer que $Z(SL_3(\mathbb{F}_2)) = \{I_3\}$ et $\mathbb{F}_2^\times = \{1\}$.

(iii) $PGL_3(\mathbb{F}_2)$ agit naturellement sur $\mathbb{P}^2(\mathbb{F}_2)$ et son action est transitive et fidèle.

(iv) Les droites de $\mathbb{F}_2^3$ sont des points de $\mathbb{P}^2(\mathbb{F}_2)$, on appelle droites de $\mathbb{P}^2(\mathbb{F}_2)$ les plans vectoriels de $\mathbb{F}_2^3$ et on note $[x]$ le point projectif correspondant à la droite $vect(x)$.

Propriété 1.1 :

$$card(G) = 168$$

Preuve : De par la remarque précédante, on sait que pour compter les éléments de G il suffit de compter les bases de $\mathbb{F}_2^3$. Or, puisque dans $\mathbb{F}_2^3 \setminus \{0\}$. être colinéaires c'est être égaux, on en déduit que pour construire une base on dispose de 7 choix pour le premier vecteur - le vecteur nul étant exclu - puis de 6 choix pour le deuxième vecteur - le vecteur nul et le premier vecteur choisi étant exclus - et enfin, 4 choix pour le dernier - le vecteur nul, les deux premiers choisis et leur somme (ou différences) étant exclus. Ce qui fait alors bien un total de 168 bases, ou encore $card(G) = 168$.

Propriété 1.2 :

G est simple.

Preuve : (Méthode dite "*d'Iwasawa*") Notons T_x le sous-groupe de G formé des transvections de droite d'image $[x]$ dans $\mathbb{P}^2(\mathbb{F}_2)$ et de I_3. Il s'agit d'un sous-groupe abélien de G vérifiant :

$$\forall g \in G : gT_xg^{-1} = T_{g(x)}$$

Supposons qu'il existe un sous-groupe propre distingué de G, N. Notons que N ne contient aucune transvection car elles sont toutes deux à deux conjuguées (dans $GL_3(\mathbb{F}_2) \simeq PSL_3(\mathbb{F}_2)$) et engendrent G et que l'on a supposé N comme sous-groupe propre.
Fixons $x \in \mathbb{F}_2^3$, remarquons que NT_x est un sous-groupe de G et $NT_x = T_xN$, car $N \lhd G$, et aussi qu'il vérifie :

$$\forall y \in \mathbb{F}_2^3 \setminus \{0\} : T_y \subset NT_x$$

En effet, considérons l'action naturelle de G et de N sur $\mathbb{P}^2(\mathbb{F}_2)$; N n'agit pas trivialement car on a supposé qu'il n'était pas réduit au neutre, on en déduit qu'il existe $n \in N$ et $[y], [z] \in \mathbb{P}^2(\mathbb{F}_2)$ distincts, tels que :

$$n.[y] = [z]$$

Montrons que N agit alors transitivement : soient $[y'], [z'] \in \mathbb{P}^2(\mathbb{F}_2)$ distincts, puisque G agit doublement transitivement sur $\mathbb{P}^2(\mathbb{F}_2)$ (simple complétion de bases), il existe $g \in G$ tel que :

$$\begin{cases} g.[y] = [y'] \\ g.[z] = [z'] \end{cases}$$

Mais alors :

$$gng^{-1}.[y'] = [z']$$

Et puisque N est distingué, on en déduit qu'il agit transitivement sur $\mathbb{P}^2(\mathbb{F}_2)$.
Soit maintenant $w \in \mathbb{F}_2^3 \setminus \{0\}$, on sait qu'il existe $k \in N$ tel que $k.[x] = [w]$, par la transitivité que l'on vient de prouver. Rappelons que $kT_xk^{-1} = T_w$, d'où : $T_w \subset NT_x$, ce qui est le résultat annoncé, duquel on déduit $NT_x = G$, car les transvections engendrent G.
On a maintenant que $G/N \simeq T_x$, car on a vu que N ne contenait aucune transvection, en particulier, il est abélien, ce dont on déduit que $D(G) \subset N$. Il ne nous reste qu'à constater que l'on peut construire une transvection comme un commutateur, ce qui contredit le fait que N est un sous-groupe propre. Par exemple, considérons les matrices et le calcul suivant :

$$\left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} ; \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Par l'absurde, on a donc prouvé que G est simple.

2 Étude de la structure d'un groupe simple à 168 éléments

À partir de cet instant, nous considérerons un groupe G, simple et de cardinal 168, nous étudierons sa structure de manière générale : ses sous-groupes de Sylow, les ordres de ses éléments, certains de ses sous-groupes propres et ses classes de conjugaison. Cela nous amènera à une propriété clef de la preuve de l'unicité du groupe simple à 168 éléments, faite dans la partie suivante.

2.1 Étude des 7-Sylow de G et des éléments d'ordre 7

Propriété 2.1.1 :

G possède 8 7-Sylow.

Preuve : Il suffit d'appliquer le théorème de Sylow sans oublier qu'il ne peut pas exister qu'un seul 7-Sylow, par simplicité de G.

Propriété 2.1.2 :

G possède 48 éléments d'ordre 7.

Preuve : Notons $\mathscr{S}_7$ l'ensemble des 7-Sylow de G et $\mathscr{O}_7$ l'ensemble des éléments d'ordre 7 de G. Puisque $card(G) = 7.3.2^3$, on a que les 7-Sylow sont d'ordre 7 donc cycliques, contenant 6 éléments d'ordre 7 et, de fait, ne s'intersectent que sur l'élément neutre. On en déduit alors que $card(\mathscr{O}_7) = card(\mathscr{S}_7).6 = 48$.

Propriété 2.1.3 :

Les éléments d'ordre 2 et 7 de G ne commutent jamais.

Preuve : Considérons le sous-groupe N, normalisateur de $P \in \mathscr{S}_7$. Remarquons que N est aussi, par définition, le stabilisateur de P sous l'action par conjugaison de G sur $\mathscr{S}_7$. Par le deuxième théorème de Sylow, on sait que cette action est transitive, et puisque $card(\mathscr{S}_7) = 8$, on en déduit : $card(N) = 21$. Or, $2 \nmid 21$, il n'y a donc pas d'élement d'ordre 2 dans N, en particulier, aucun élément d'ordre 2 ne commute aux éléments de P et plus généralement aux éléments d'ordre 7 de G, cette preuve étant valable pour n'importe quel 7-Sylow.

2.2 Étude des 3-Sylow de G et des éléments d'ordre 3

Propriété 2.2.1 :

G possède 28 3-Sylow

Preuve : Notons $\mathscr{S}_3$ l'ensemble des 3-Sylow de G et $\mathscr{O}_3$ l'ensemble des éléments d'ordre 3 de G. Le deuxième théorème de Sylow appliqué à G nous donne : $card(\mathscr{S}_3) \in \{4;7;28\}$. Pour éliminer les deux premières possibilités, réutilisons les normalisateurs de 7-Sylow :
Soient $P, Q \in \mathscr{S}_7$ (distincts) et N (resp. M) le normalisateur de P (resp. Q).

Lemme 2.2.1 :

N et M sont non cycliques et contiennent chacun 6 éléments d'ordre 7 et 14 d'ordre 3.

Preuve : Par l'action de G par conjugaison sur $\mathscr{S}_7$ et par le fait que G est simple, on en déduit un plongement de G dans $\mathfrak{S}_8$ (car G n'agit pas trivialement, selon le théorème de Sylow). Or il n'existe pas d'élément d'ordre 21 dans $\mathfrak{S}_8$ [1], on en déduit donc que N et M ne sont pas cycliques. De plus, le deuxième théorème de Sylow nous donne qu'ils ne contiennent chacun qu'un 7-Sylow, et puisque que $card(N) = card(M) = 3.7$, on en conclut qu'ils possèdent chacun 6 éléments d'ordre 7 et 14 d'ordre 3.

1. On peut facilement calculer les ordres des éléments dans les groupes symétriques. Il suffit d'utiliser la décomposition (unique) en cycles de supports disjoints, on prouve alors aisément que l'ordre d'un élément est le *ppcm* des ordres de ses cycles. Ici, par exemple, on ne peut avoir d'élément d'ordre 21 dans $\mathfrak{S}_8$ car un tel élément devrait être le produit d'un 7-cycle et d'un 3-cycle à supports disjoints, ce qui ne se peut car requiert 10 éléments pour construire les supports, alors que l'on en dispose que de 8.

Reprenons la preuve de la propriété. Puisque Q et P sont distincts, il en va de même pour N et M car ils ne contiennent qu'un seul sous-groupe de cardinal 7, on en déduit aussi que $card(N \cap M) \in \{1;3\}$. Dans tous les cas, on observe qu'il existe alors au moins 26 éléments d'ordre 3 dans G, ce dont on déduit que $card(\mathscr{S}_3) = 28$ car les 3-Sylow sont d'ordre 3, donc cycliques, donc ne s'intersectent qu'en l'élément neutre et comptent chacun 2 éléments d'ordre 3. On en déduit alors aussi la propriété suivante.

Propriété 2.2.2 :

G possède 56 éléments d'ordre 3.

Propriété 2.2.3 :

Les éléments d'ordre 2 et 3 de G ne commutent jamais.

Preuve : Soient $K \in \mathscr{S}_3$ et V son normalisateur. Par les mêmes types de remarques qu'avec les normalisateurs de 7-Sylow, on a que $card(V) = 6$. Montrons que V est non cyclique. On en déduira alors qu'il est isomorphe à $\mathfrak{S}_3$ [2], dans lequel les éléments d'ordre 2 et 3 ne commutent pas, ce qui nous donnera alors le résultat annoncé. Procédons par l'absurde, supposons que V est cyclique. Puisque les 3-Sylow sont isomorphes car conjugués [3], on en déduit qu'ils sont tous cycliques. Remarquons aussi que les normalisateurs de deux 3-Sylow différents sont distincts car ils ne contiennent chacun qu'un seul sous-groupe de cardinal 3, ils ne peuvent donc pas s'intersecter sur un élément d'ordre 6. On en déduit alors qu'il existe 56 éléments d'ordre 6 dans G. En résumé, on connaît déjà 161 éléments de G puisque l'on a dénombré 56 éléments d'ordre 6, 56 éléments d'ordre 3, 48 éléments d'ordre 7 et le neutre. Or on sait qu'il existe au moins deux 2-Sylow dans G - car il en existe au moins un et qu'il ne peut être seul sinon il serait distingué ce qui contredit l'hypothèse de simplicité de G - et qu'ils sont d'ordre 8, ce qui contredit le fait que $card(G) = 168$. On en déduit alors que V ne peut être cyclique.

2.3 Ordres des éléments de G

Propriété 2.3.1 :

$$G = \mathscr{O}_1 \sqcup \mathscr{O}_2 \sqcup \mathscr{O}_3 \sqcup \mathscr{O}_4 \sqcup \mathscr{O}_7 \sqcup \mathscr{O}_8$$

Où $\mathscr{O}_i$ est l'ensemble des éléments d'ordre i dans G.

Preuve : Comme on l'a déjà dit, on peut plonger G dans $\mathfrak{S}_8$. On en déduit alors que l'ordre maximal d'un élément de G est inférieur à 15, car il s'agit de l'ordre maximal d'un élément de $\mathfrak{S}_8$. Mais du fait que $5 \nmid card(G)$ et qu'il n'existe ni d'élément d'ordre 14 ni d'élément d'ordre 13 dans $\mathfrak{S}_8$, on a alors que l'ordre maximal d'un élément de G est majoré par 12. De plus, par la preuve de la propriété 2.2.3, on sait qu'il n'existe pas d'élément d'ordre 6, donc pas non plus d'élément d'ordre 12. Par suite, les diviseurs de 168 inférieurs strictement à 12 étant $\{1;2;3;4;6;7;8\}$, on en déduit le résultat.

Remarques : (i) Grâce à ce dernier résultat, on sait maintenant que pour compter les éléments de G il nous suffira de compter les éléments intervenant dans les sous-groupes de Sylow de G.

(ii) On verra plus loin qu'il n'existe, en fait, aucun élément d'ordre 8.

2.4 Étude des 2-Sylow et des éléments d'ordre 2, 4 et 8

Propriété 2.4.1 :

G possède 21 2-Sylow.

2. Il n'existe que deux groupes à 6 éléments à isomorphisme près, dont l'un étant $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et l'autre étant $\mathfrak{S}_3$
3. La conjugaison par un élément de G est un automorphisme de G dont l'inverse est la conjugaison par l'élément inverse.

Preuve : Par la remarque précédante, on sait que $card\left(\bigcup_{K\in\mathscr{S}_2} K\setminus\{e_G\}\right) = 63$ et le deuxième théorème de Sylow nous donne : $card(\mathscr{S}_2)\in\{1;3;7;21\}$, ce qui force le résultat.

Propriété 2.4.2 :

Les 2-Sylow ne sont pas abéliens, en particulier, G ne possède pas d'éléments d'ordre 8, soit :

$$G = \mathscr{O}_1 \sqcup \mathscr{O}_2 \sqcup \mathscr{O}_3 \sqcup \mathscr{O}_4 \sqcup \mathscr{O}_7$$

Preuve : Procédons par l'absurde : supposons que les 2-Sylow sont abéliens. Soient $D, D' \in \mathscr{S}_2$ (distincts) tels que : $D\cap D' \neq \{e_G\}$. De tels sous-groupes existent car $card\left(\bigcup_{K\in\mathscr{S}_2} K\setminus\{e_G\}\right) = 63$ et qu'il n'existe que 21 2-Sylow (qui sont d'ordre 8). Soit donc $x\in(D\cup D')\cap\mathscr{O}_2$ (on peut l'exiger d'ordre 2, car s'il ne l'est pas, une de ses puissances l'est). On observe que $D\cup D'\subset Z(x)$ puisqu'ils sont abéliens. Or, rappelons-nous qu'aucun élément d'ordre 3, ou 7, ne commute avec un élément d'ordre 2, ce dont on déduit : $card(Z(x))\in\{1;2;4;8\}$. Mais cela contredit : $D\cup D'\subset Z(x)$, car $card(D\cup D') > 8$. On en conclut que les 2-Sylow ne sont pas abéliens, donc sont non cycliques, donc ne possèdent pas d'élément d'ordre 8, et enfin, G non plus car sinon il serait contenu dans l'un des 2-Sylow d'après le deuxième théorème de Sylow.

Propriété 2.4.3 :

G possède 42 éléments d'ordre 4 et 21 d'ordre 2.

Preuve : Soit $D\in\mathscr{S}_2$, puisqu'il est de cardinal 8 et non abélien, on sait qu'il possède des éléments d'ordre 4. Soit ρ l'un d'eux. On a $\rho^2\in\mathscr{O}_2$, on sait alors que $card(Z(\rho^2))\in\{4;8\}$ (car il contient déjà les autres puissances de ρ), on en déduit alors que sa classe de conjugaison est de cardinal 21 ou 42. Par suite, il existe alors au moins 21 carrés d'éléments d'ordre 4 dans G (par simple calcul, on peut montrer que c'est une caractéristique conservée par conjugaison), et puisque $\rho^2 = (\rho^3)^2$, il existe alors au moins 42 éléments d'ordre 4. Mais de part :

$$63 = card\left(\bigcup_{K\in\mathscr{S}_2} K\setminus\{e_G\}\right) = card(\mathscr{O}_2\sqcup\mathscr{O}_4)$$

On conclut que $card(\mathscr{O}_2) = 21$ et $card(\mathscr{O}_4) = 42$.

Remarque : Cette preuve nous donne aussi que $\mathscr{O}_2$ et $\mathscr{O}_4$ sont des classes de conjugaison. Elle nous donne encore que si $x\in\mathscr{O}_2$ alors $Z(x)\in\mathscr{S}_2$.

Propriété 2.4.4 :

Les 2-Sylow de G sont isomorphes au groupe diédral à 8 éléments, D_8.

Preuve : Soit $D\in\mathscr{S}_2$. Puisqu'il doit contenir le neutre et au moins un élément d'ordre 2 (premier théorème de Sylow), on en déduit que D possède au plus 6 éléments d'ordre 4.
Supposons qu'il en possède exactement 6. On a alors que leurs carrés sont le seul élément d'ordre 2 de D, inversement, pour chaque élément d'ordre 2 de G, on lui compte 6 "racines carrées", ce qui contredit le résultat de la propriété précédente. D a alors au plus 4 éléments d'ordre 4.
Soient $(y,x)\in\mathscr{O}_4\times\mathscr{O}_2$ tels que $x\neq y^2$, ce qui est possible car $card(\mathscr{O}_2)\geqslant 3$. On a $card(<y,x>)\in\{4;8\}$.
Supposons que $card(<y,x>) = 4$, alors $<y,x>$ est abélien et est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, car contient un élément

d'ordre 4. Ce qui est impossible du fait de $x \neq y^2$.
Donc $card(< y,x >) = 8$, ou encore $< y,x >= D$. Or :

$$\{e_G\,;\, x\,;\, y\,;\, y^2\,;\, y^3\,;\, xy\,;\, xy^2\,;\, xy^3\} \subset < y,x >$$

Par cardinalité, on en déduit que l'on a la description complète de $< y,x >= D$. De plus, on observe que $yx = xy^{-1}$ car $< y >$ est d'indice 2 donc distingué, que xyx est forcément d'ordre 4 et ne peut être y car les 2-Sylow ne sont pas abéliens (propriété 2.4.2).

2.5 Classes de conjugaison de G

Propriété 2.5.1 :

Les classes de conjugaison de G sont $\mathscr{O}_1$, $\mathscr{O}_2$, $\mathscr{O}_3$, $\mathscr{O}_4$, $\mathscr{C}_1$ et $\mathscr{C}_2$. Où $\mathscr{C}_1 \sqcup \mathscr{C}_2 = \mathscr{O}_7$ et où $card(\mathscr{C}_i) = 24$.

Preuve : Rappelons que puisque deux éléments qui n'ont pas le même ordre ne peuvent pas être conjugués, on en déduit que la partition de G en classes de conjugaison est plus fine que :

$$G = \mathscr{O}_1 \sqcup \mathscr{O}_2 \sqcup \mathscr{O}_3 \sqcup \mathscr{O}_4 \sqcup \mathscr{O}_7$$

Mais on a déjà vu que $\mathscr{O}_2$ et $\mathscr{O}_4$ étaient des classes de conjugaison (remarque sur la preuve de la propriété 2.4.3). Étudions alors les cas de $\mathscr{O}_3$ et $\mathscr{O}_7$.

Le cas de $\mathscr{O}_3$:
Soit $x \in \mathscr{O}_3$, notons N le normalisateur de $< x >$. On sait que $N \simeq \mathfrak{S}_3$ (preuve de la propriété 2.2.3). Et par définitions : $Z(x) \subset N$. Or, dans $\mathfrak{S}_3$, aucun élément ne commute aux éléments d'ordre 3, si ce n'est leurs puissances. On en déduit que $card(Z(x)) = 3$. Par suite, on trouve que l'orbite de x sous l'action par conjugaison de G sur ses éléments, est de cardinal 56. On en conclut que $\mathscr{O}_3$ est une classe de conjugaison.

Le cas de $\mathscr{O}_7$:
Soit $u \in \mathscr{O}_7$, notons P le normalisateur de $< u >$. On a toujours : $Z(u) \subset P$. Or, P n'est pas cyclique et :

$$\forall \sigma, \tau \in (P \cap \mathscr{O}_7) \times (P \cap \mathscr{O}_3) : \; < \sigma, \tau >= P$$

D'où :

$$\forall \sigma, \tau \in (P \cap \mathscr{O}_7) \times (P \cap \mathscr{O}_3) : [\sigma;\tau] \neq e_G$$

On en déduit alors que : $card(Z(u)) = 7$. Mais alors : $card(G.u) = 24$. Et plus généralement, $\mathscr{O}_7$ est union de deux classes de conjugaison d'ordre 24 : $\mathscr{C}_1$ et $\mathscr{C}_2$.

2.6 Les sous-groupes de Klein de G

Cette partie est spécifique à un type de sous-groupes de G qui nous servirons ensuite à démontrer l'unicité du groupe simple à 168 éléments.

Définition : On appelle sous-groupe de Klein de G, tout sous-groupe d'ordre 4 non cyclique de G. On notera $\mathscr{K}$ l'ensemble de ces sous-groupes.

Propriété 2.6.1 :

G possède 14 sous-groupes de Klein.

Preuve : Soit $K \in \mathscr{K}$. Puisqu'il est d'ordre 4, il est abélien, en particulier, il est l'intersection des centralisateurs de ses éléments d'ordre 2 qui sont des 2-Sylow, distincts, car n'ont qu'un seul élément d'ordre 2 dans leurs centres (propriété du groupe diédral). Inversement, toujours par les propriétés du groupe diédral, chaque 2-Sylow possède deux sous-groupes d'ordre 4 non cycliques. On en déduit alors : $card(\mathscr{K}).3 = card(\mathscr{S}_2).2$, soit $card(\mathscr{K}) = 14$.

3 Unicité du groupe simple d'ordre 168

3.1 Action particulière de G

Lemme 3.1.1 :

$\mathscr{K}$ est l'union de deux orbites de cardinal 7, de l'action de G par conjugaison sur ses sous-groupes.

Preuve : Soit $K \in \mathscr{K}$, notons N le normalisateur de K, qui est aussi son stablisateur (par définitions). On a évidemment : $\left(\bigcup_{u \in K \setminus \{e_G\}} Z(u) \right) \subset N$, ce dont on déduit que $card(N) \geqslant 16$ et $8 \mid card(N)$. Par suite, N est de cardinal 24, 56 ou 168. Or, si $card(N) = 168$, cela signifie que K est distingué dans G, ce qui est impossible (K étant un sous-groupe propre de G). On a alors que $card(orb(K)) \in \{3;7\}$. Or, si une orbite d'un sous-groupe de Klein était de cardinal 3, on ne pourrait plus faire une partition de l'ensemble des sous-groupes de Klein, qui compte 14 éléments, avec des sous-ensembles de cardinaux 3 ou 7. On en déduit alors que $card(orb(K)) = 7$, ce qui donne le résultat.

Théorème 3.1.1 :

Tout groupe simple de cardinal 168 agit transitivement et fidèlement sur un ensemble à 7 éléments

Preuve : D'après le lemme précédent, tout groupe simple de cardinal 168 agit transitivement sur une des deux orbites que constituent l'ensemble des sous-groupes de Klein et qui possède 7 éléments. La fidélité est juste conséquence de la simplicité de G (puisqu'il n'agit pas trivialement).

3.2 Théorème d'unicité

Dans cette section on considère juste le groupe G (toujours supposé simple et à 168 éléments) agissant transitivement et fidèlement sur un ensemble à 7 éléments, $\mathscr{S}$, ce que l'on sait maintenant être toujours possible. On utilisera abondemment l'identification de G à un sous-groupe de $\mathfrak{S}_7$ pour cette action et pour une autre action que l'on introduira plus loin.

Propriétés 3.2.1 :

(i) $G \subset \mathfrak{A}_7$, en particulier, les éléments d'ordre 2 de G sont des bitranspositions et les éléments d'ordre 4 sont des produits d'un 4-cycle et d'une transposition à supports disjoints.

(ii) Il existe des 7-cycles dans G.

(iii) Il n'existe pas de 3-cycles dans G, en particulier, les éléments d'ordre 3 de G sont des bi-3-cycles.

Preuve : (i) Si G n'est pas inclu dans $\mathfrak{A}_7$ alors $G \cap \mathfrak{A}_7$ est un sous-groupe d'indice 2 de G, donc distingué, non trivial, et différent de G, ce qui contredit la simplicité de G. On en déduit alors immédiatement que les éléments d'ordre 2 de G sont des bitranspositions et que les éléments d'ordre 4 sont des produits de 4-cycles et de transpositions à supports disjoints.

(ii) Par le premier théorème de Sylow, on sait que G possède des éléments d'ordre 7, mais un élément de cet ordre dans $\mathfrak{S}_7$ est nécessairement un 7-cycle.

(iii) Puisque $\mathfrak{A}_7$ est engendré par n'importe quel couple formé d'un 7-cycle et d'un 3-cycle et que $G \subsetneq \mathfrak{A}_7$ (par le point (i) et par cardinalité), on a alors que G ne contient aucun 3-cycle. Mais, toujours par le premier théorème de Sylow, on sait que G possède des éléments d'ordre 3, or, les seuls éléments d'ordre 3 qui ne sont pas des 3-cycles dans $\mathfrak{S}_7$ sont les bi-3-cycles.

Notation : On notera $\mathscr{D}$ l'ensembles des 3-parties de points fixes d'éléments d'ordre 2 de G.

Propriétés 3.2.2 :

(i) Pour tout $s, t \in \mathscr{S}$ distincts, il existe un unique $D \in \mathscr{D}$ tel que $\{s;t\} \subset D$.

(ii) Pour tout $D, D' \in \mathscr{D}$ distincts, il existe un unique $s \in \mathscr{S}$ tel que $D \cap D' = \{s\}$.

Preuve :(i) Soit $s \in \mathscr{S}$, par la transitivité de l'action de G sur $\mathscr{S}$, on a $card(G_s) = 24$ où G_s est le stabilisateur de s. Notons que si $t \in \mathscr{S} \setminus \{s\}$, alors $G_s \neq G_t$, en effet, il suffit de remarquer qu'il existe des éléments d'ordre 3 dans G_s, puisque $card(G_s) = 3.2^3$, et que ces éléments ont un support de cardinal 6 (propriété 3.2.1.(iii)), ils ne peuvent donc pas fixer s. Notons $I = G_s \cap G_t$. Remarquons, qu'un élément de I a au plus un support de cardinal 5, ce dont on déduit qu'il n'existe pas d'élément d'ordre 3, 4 ou 7 dans I, par cardinalité de leur support (propriété 3.2.1.(i) et (iii)). De plus, I n'est pas trivial car sinon G possèderait au moins 24^2 éléments. On en déduit alors qu'il n'est formé que du neutre et de bitranspositions. Notons $\Sigma = \mathscr{S} \setminus \{s;t\} = \{p_1;p_2;p_3;p_4;p_5\}$. Par définition, on a que I s'identifie à un sous-groupe de $\mathfrak{S}_\Sigma$, or $card(\Sigma) = 5$ et $5 \nmid card(I)$ (car il s'agit d'un sous-groupe de G), donc I ne peut pas agir transitivement sur Σ. Supposons que I ne laisse fixe aucun point de Σ, alors, il existerait une orbite de cardial 2 et une autre de 3. Supposons, sans perte de généralité que celle de cardinal 3 est : $\{p_1;p_2;p_3\}$. Il existe alors un élément de I de la forme : $(p_1\ p_2)(p_4\ p_5)$ et un autre de la forme : $(p_1\ p_3)(p_4\ p_5)$ (quitte à permuter les points p_1, p_2 et p_3). De fait $(p_3\ p_2\ p_1) \in I$ ce qui est impossible. On en déduit que I a un unique point fixe, w, sur Σ, et puisqu'il est formé de bitranspositions et du neutre, on a :

$$\{s;t;w\} \in \mathscr{D}$$

(ii) La preuve précédente nous donne que deux éléments distincts de $\mathscr{D}$, D_1 et D_2, ont au plus un point d'intersection. Supposons qu'ils n'en ont pas. Ils sont (respectivement) les ensembles de points fixes de u et v, deux bitranspositions de G. Soit $\{q_1\} = \mathscr{S} \setminus (D_1 \cup D_2)$, notons $u(q_1) = q_2$ et $v(q_1) = q_3$. Puisqu'il s'agit de bitranspositions, elles sont de la forme : $u = (q_1\ q_2)(q_4\ q_5)$ et $v = (q_1\ q_3)(q_6\ q_7)$. Ce qui donne : $uv = (q_3\ q_2\ q_1)(q_4\ q_5)(q_6\ q_7)$, qui est un élément d'ordre 6, or, on a vu qu'il n'en existait pas dans G (preuve de la propriété 2.2.3).

Propriété 3.2.3 :

$\mathscr{D}$ est de cardinal 7 et l'action de G sur $\mathscr{S}$ induit une action transitive et fidèle de G sur $\mathscr{D}$

Preuve : En préliminaire, remarquons que tous les éléments de $\mathscr{S}$ interviennent dans les 3-parties de points fixes comme le montre le point (i) des dernières propriétés. Par le point (i) toujours, on sait qu'il existe au moins un élément dans $\mathscr{D}$, notons le D. Soit $a \in D$, puisque tous les éléments de $\mathscr{S}$ interviennent et que tout couple $\{a\,;\,b\}$ où $b \in \mathscr{S}$ doit être contenu dans un unique élément de $\mathscr{D}$, on en déduit qu'il existe exactement 3 éléments de $\mathscr{D}$ qui contiennent a (D inclu). On observe alors aussi que D rencontre en un point unique (propriété (ii)) exactement 6 autres éléments (distincts) de $\mathscr{D}$; en effet, si D est coupé en a par une droite D^1 et en un certain b par une droite D^2 alors D^1 et D^2 sont distinctes d'après la propriété (i). Par suite, $card(\mathscr{D}) \geqslant 7$. Mais cela nous dit aussi que si $card(\mathscr{D}) > 7$, alors il existe deux éléments distincts de $\mathscr{D}$ qui ne s'intersectent pas, ce qui contredit la propriété (ii). Finalement : $card(\mathscr{D}) = 7$. En ce qui concerne l'action de G sur $\mathscr{D}$ il suffit de considérer l'action induite par celle sur les éléments de $\mathscr{S}$; en effet, si $D \in \mathscr{D}$ et $g \in G$, il existe k, une bitransposition de G dont l'ensemble des points fixes est D. Considérons alors gkg^{-1}, il s'agit bien d'une bitransposition (la décomposition en cycles disjoints étant un invariant de conjugaison) dont l'ensemble des points fixes est $g(D)$, de fait $g(D) \in \mathscr{D}$, d'où l'action.
Enfin, pour avoir la transitivité de cette action, il suffit de remarquer que si D^1 et D^2 sont deux ensembles de points fixes d'éléments d'ordre 2 de G : u et v (respectivement), alors, pour envoyer D^1 sur D^2, il suffit de considérer l'action sur $\mathscr{D}$ de l'élément de G qui conjugue u à v (on sait qu'il existe propriété 2.5.1). La fidélité de l'action est donnée par le fait que G est simple et n'agit pas trivialement.

Remarque : Maintenant, nous disposons de deux points de vue sur l'action de G sur $(\mathscr{S},\mathscr{D})$, cela s'avèrera particulièrement commode dans la partie suivante.

Lemme 3.2.1 :

Il existe une structure de $\mathbb{F}_2$-espace vectoriel de dimension 3 sur $\mathscr{S}\cup\{O\}$, où $O\notin\mathscr{S}$

Preuve :On définit la loi interne par :

$\forall s\in\mathscr{S} : s+O=O+s=s$

$\forall s\in\mathscr{S}\cup\{O\} : s+s=O$

$\forall s,t\in\mathscr{S}$ on pose $s+t$ comme l'unique point de $\mathscr{S}$ tel que : $\{s\,;t\,;s+t\}\in\mathscr{D}$

On en déduit que O est l'élément neutre, que tout élément différent du neutre est d'ordre 2, donc qu'il a un unique inverse étant lui même, puisque cette loi est commutative. Vérifions qu'elle est bien associative :
Soient s, t et r appartenant à $\mathscr{S}$ tels que $\{s\,;t\,;r\}\notin\mathscr{D}$. Par définitions, on a :

$$\{r\,;s+t\,;r+s+t\}\in\mathscr{D}$$

$$\{r\,;t\,;r+t\}\in\mathscr{D}$$

Par la propriété 3.2.2.(ii) de $(\mathscr{S},\mathscr{D})$, on en déduit :

$$\{r\,;s+t\,;r+s+t\}\cap\{r\,;t\,;r+t\}=\{r\}$$

En particulier : $r+t\neq s+r+t$. Notons D l'unique élément de $\mathscr{D}$ qui contienne s et $r+t$, et D' l'élément $\{r\,;s+t\,;r+s+t\}$. Par ce que l'on a fait, on sait qu'alors, D et D' se coupent forcément en $r+s+t$, ce qui est le résultat attendu.
On dispose alors d'un groupe abélien pour $+$, dont tous les éléments, sauf le neutre, sont d'ordre 2 et qui est de cardinal 8. Il ne reste qu'à définir la loi externe : "." pour en faire un $\mathbb{F}_2$-espace vectoriel de dimension 3. Par les relations déjà écrites, nons n'avons d'autre choix que :

$$\forall s\in\mathscr{S}\cup\{O\} : \begin{cases} 1.s=s \\ 0.s=O \end{cases}$$

La vérification de la distributivité étant évidente, on en conclut le théorème.

Théorème 3.2.1 :

Il n'existe qu'un seul groupe simple à 168 éléments et à isomorphisme près.

Preuve : D'après la structure d'espace vectoriel que l'on a mise sur $\mathscr{S}\cup\{O\}$, on en déduit que P est un plan de $\mathscr{S}\cup\{O\}$ si et seulement si $P\in\mathscr{D}$. Voyons qu'alors l'action de G se traduit comme une action par homographies sur $\mathbb{P}(\mathscr{S}\cup\{O\})$.
Pour ce faire, il suffit de remarquer qu'une application est une homographie si et seulement si elle est une bijection sur l'ensemble des points (projectifs), ici en bijection avec $\mathscr{S}$, et qu'elle induit une bijection sur l'ensemble des droites (projectives), ici $\mathscr{D}$. Or ces résultats ont déjà été montrés pour tous les éléments de G (propriété 3.2.3). Par suite, puisque l'on a évidemment une bijection entre $\mathbb{P}(\mathscr{S}\cup\{O\})$ et $\mathbb{P}^2(\mathbb{F}_2)$, et puisque l'action de G est fidèle, on en déduit un plongement de G dans $PGL_3(\mathbb{F}_2)$. Mais par les remarques et l'étude de cardinalité de la partie 1, cela nous donne :

$$G\simeq PSL_3(\mathbb{F}_2)$$

Autrement dit, $PSL_3(\mathbb{F}_2)$ est l'unique groupe simple à 168 éléments, à isomorphisme près.

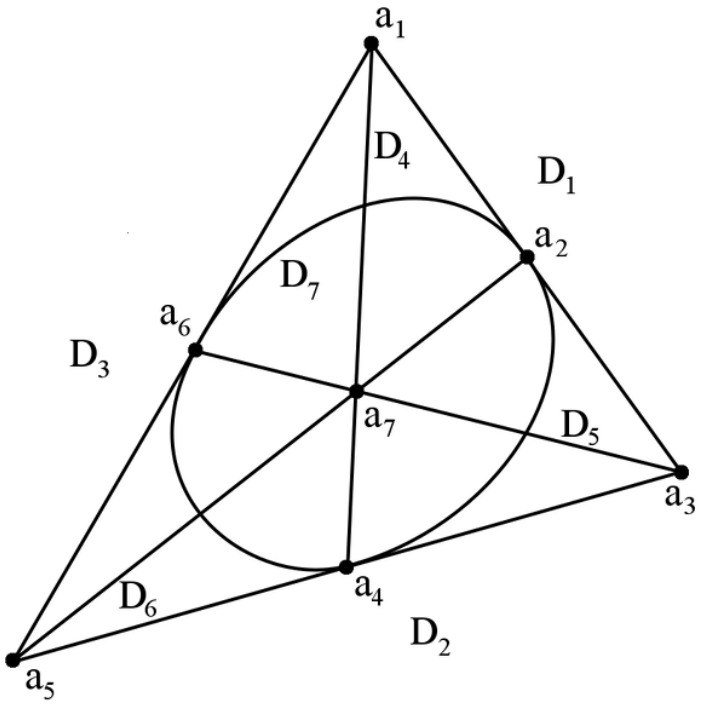
Remarque : À partir de maintenant, grâce à une représentation de $(\mathscr{S},\mathscr{D})$ on pourra expliciter des éléments de G, car on sait qu'il s'agit exactement des éléments qui induisent une bijection à la fois sur $\mathscr{S}$ et sur $\mathscr{D}$.

4 Les sous-groupes de G

Forts de notre résultat d'unicité, complétons notre étude de la structure du groupe simple à 168 éléments en commençant par l'étude de ses sous-groupes. Pour ce faire, et en accord avec notre dernière remarque, nous utiliserons la donnée de $(\mathscr{S}, \mathscr{D})$ suivante :

$$\mathscr{S} = \{a_i \mid i \in [\![1\,;7]\!]\}$$

$$\mathscr{D} = \{D_1 = \{a_1\,;a_2\,;a_3\}\,; D_2 = \{a_3\,;a_4\,;a_5\}\,; D_3 = \{a_5\,;a_6\,;a_1\}\,;$$
$$D_4 = \{a_1\,;a_4\,;a_7\}\,; D_5 = \{a_3\,;a_6\,;a_7\}\,; D_6 = \{a_2\,;a_7\,;a_5\}\,; D_7 = \{a_2\,;a_4\,;a_6\}\}$$



4.1 Zoologie des sous-groupes de G

Propriété 4.1.1 :

G ne possède aucun sous-groupe d'ordre 14, 28, 42, 56 ou 84.

Preuve : Dans le cas d'un sous-groupe d'ordre 84, il suffit de voir que ce sous-groupe serait distingué car d'indice 2, ce qui est impossible par simplicité de G.
Pour un sous-groupe H d'ordre 14, 28 ou 42, on sait qu'il existe un unique 7-Sylow dans H, et puisque le cardinal de H est pair, on en déduit qu'il existe un élément d'ordre 2 dans le normalisateur dudit 7-Sylow, ce que l'on sait être faux (propriété 2.1.3), autrement dit, un tel H n'existe pas.
Dans le cas d'un sous-groupe H à 56 éléments, soit il possède un unique 7-Sylow comme sous-groupe, et, de fait, l'argument d'au-dessus donne le résultat attendu ; soit, il possède comme sous-groupe un unique 2-Sylow de G. Or, puisqu'il y a 21 2-Sylow dans G et qu'il sont tous conjugués (théorème de Sylow), on en déduit que le normalisateur d'un 2-Sylow est lui même, ainsi H, ne contenant qu'un seul de ces sous-groupes, serait inclu dans son normalisateur (par définitions), ce qui est impossible par cardinalité. On en déduit donc bien que G ne possède pas de sous-groupe d'ordre 56.

Propriété 4.1.2 :

Il existe dans G des sous-groupes d'ordre 3, 7 et 8 qui sont les sous-groupes de Sylow, 2 et 4 qui sont les sous-groupes des 2-Sylow, 6 et 21 qui sont les normalisateurs des 3-Sylow et des 7-Sylow, respectivement.

Preuve : Ici, il ne reste à prouver que le fait que les sous-groupes d'ordre 6 et 21 sont forcément des normalisateurs de 3-Sylow et de 7-Sylow, respectivement. Pour cela, il suffit d'observer que de tels sous-groupes possèdent un unique tel sous-groupe de Sylow, donc il est distingué, ces sous-groupes sont alors des sous-groupes des normalisateurs, et par cardinalité, on en déduit qu'ils leur sont égaux.

Propriété 4.1.3 :

Il existe des sous-groupes d'ordre 24 dans G, et il s'agit exactement des stabilisateurs des éléments de $\mathscr{S}$ ou $\mathscr{D}$ sous l'action de G.

Preuve : Puisque l'on sait que l'action de G sur $\mathscr{S}$ et sur $\mathscr{D}$ est transitive, on en déduit immédiatement que les stabilisateurs sont d'ordre 24. Vérifions la réciproque.
Soit H un sous-groupe de G d'ordre 24. Si H fixe un élément de $\mathscr{S}$, il n'y a rien à faire, supposons donc qu'il n'en fixe aucun. Notons $Orb(H,\mathscr{S})$ l'ensemble des orbites de l'action de H sur $\mathscr{S}$. Puisque : $\forall o \in Orb(H,\mathscr{S})$: $card(o) \mid card(H)$, on a alors : $card(o) \in \{1\,;2\,;3\,;4\,;6\}$. Mais, par notre hypothèse, les cas 1 et 6 sont exclus car ils signifient exactement que H a un point fixe. On en déduit que la partition en orbites de $\mathscr{S}$ sous l'action de H est une partition d'un ensemble de 7 éléments avec des parties de cardinal 2, 3 ou 4. Par imparité, on a déjà qu'il existe $w \in Orb(H,\mathscr{S})$ où $card(w) = 3$, notons $w' = [\![1\,;7]\!]\backslash w$. On a alors que w' est soit une orbite, soit l'union disjointe de deux orbites de cardinal 2, mais puisqu'il existe des éléments d'ordre 4 dans G, donc dans H (par cardinalité il contient au moins un des 2-Sylow de G), soit σ un tel élément, puisqu'il induit forcément une orbite d'ordre 4, on en conclut alors que $w' \in Orb(H,\mathscr{S})$. Mais l'on a aussi que σ^2 est une bistranposition de support w', ou encore, d'ensemble de points fixes w ; w est alors un élément de $\mathscr{D}$ laissé stable par H, ce qui est le résultat attendu.

Propriété 4.1.4 :

Les stabilisateurs d'éléments de $\mathscr{S}$ ou $\mathscr{D}$ dans G sont isomorphes à $\mathfrak{S}_4$, en particulier, G possède des sous-groupes d'ordre 12.

Preuve : Soit G_a le stabilisateur de $a \in \mathscr{S}$, on peut supposer, sans perte de généralité, que $a = a_1$, ce qui nous permettra de faire des calculs explicites. On sait déjà que G_a est d'ordre 24, montrons que l'on peut le plonger dans $\mathfrak{S}_4$, cela nous donnera alors le résultat annoncé, car les considérations que nous ferons sur les éléments de $\mathscr{S}$ sont aussi valables sur les éléments de $\mathscr{D}$.
Observons l'action de G_{a_1} sur $\mathscr{D}$. Remarquons qu'il existe exactement trois éléments, D_1, D_3, D_4, qui contiennent a_1, et puisque G_{a_1} fixe a_1, on en déduit que G_{a_1} laisse stable $\{D_1\,;D_3\,;D_4\}$ mais aussi son complémentaire : $\{D_2\,;D_5\,;D_6\,;D_7\}$. Montrons que l'action de G_a sur $\{D_2\,;D_5\,;D_6\,;D_7\}$ est fidèle. En effet, supposons qu'il existe $g \in G_a$ tel que : $g.D_i = D_i\ \forall i \in \{2\,;5\,;6\,;7\}$, alors en particulier : $g.D_2 = D_2$, donc g agit sur $\{a_3\,;a_4\,;a_5\}$. Remarquons que si $g.a_3 \neq a_3$, alors $g.D_5 \neq D_5$, ce qui contredit nos hypothèses, donc $g.a_3 = a_3$. Le même type de raisonnement étant possible sur les autres éléments, on en déduit que g agit trivialement sur $\mathscr{S}$, et donc il s'agit du neutre, par fidélité de l'action de G sur $\mathscr{S}$. On en déduit que G_{a_1} agit fidèlement sur un ensemble à 4 éléments, donc on peut le plonger dans $\mathfrak{S}_4$, ce qui donne le résultat.

Lemme 4.1.1 :

Les sous-groupes d'ordre 24 de G ne s'intersectent jamais en un sous-groupe d'ordre 12.
Plus précisément, si H et K sont les stabilisateurs de deux éléments (distincts) de $\mathscr{S}$ ou de deux éléments de $\mathscr{D}$, alors $H \cap K$ est un sous-groupe de Klein. Si l'un est un stabilisateur d'un élément a de $\mathscr{S}$ et l'autre d'un élément D de $\mathscr{D}$, alors $H \cap K$ est le normalisateur d'un 3-Sylow (resp. un 2-Sylow) si $a \notin D$ (resp. si $a \in D$).

Preuve : (i) Supposons, sans perte de généralité, que $H = G_{a_1}$ et $K = G_{a_2}$. Notons $I = H \cap K$. D_1 est l'unique élément de $\mathscr{D}$ contenant a_1 et a_2, on en déduit que $I \subset G_{D_1}$. De plus, on sait que I agit sur $\mathscr{D}$, et, puisque ses

éléments fixent 2 éléments de $\mathscr{S}$ (en fait 3), on sait alors que ses éléments ne peuvent être que le neutre et des bitranspositions, pour des questions de cardinalité de support. Il nous suffit alors de remarquer que l'on peut trouver des éléments de I explicitement, et on en déduit qu'il s'agit d'un sous-groupe de Klein, prendre par exemple : $(a_4\ a_5)(a_6\ a_7)$ qui induit la bijection : $(D_3\ D_4)(D_6\ D_7)$ et $(a_4\ a_6)(a_5\ a_7)$ qui induit la bijection : $(D_2\ D_5)(D_3\ D_4)$.

(ii) Si H et K sont des stabilisateurs d'éléments de $\mathscr{D}$, on peut réécrire une preuve similaire.

(iii) Supposons maintenant, sans perte de généralité, que $H = G_a$ et $K = G_D$ pour $a \in \mathscr{S}$ et $D \in \mathscr{D}$.

Premier cas : si $a \notin \mathscr{D}$. Voyons qu'alors il ne peut exister d'élément d'ordre 4 dans I, de par la cardinalité de leur support (propriété 3.2.1.(i)). On en déduit alors qu'il n'existe pas de 2-Sylow de G dans I, et par suite, $8 \nmid card(I)$, soit : $card(I) \in \{1\,;\,6\,;\,12\}$. Supposons que $card(I) = 12$, on a alors que I possède 1 ou 4 sous-groupes de Sylow pour le nombre premier 3, mais puisqu'un 3-Sylow de I est un 3-Sylow de G et que le normalisateur dans G d'un tel sous-groupe est de cardinal 6, on en déduit que I possède 4 3-Sylow. De fait, il a 8 éléments d'ordre 3, or ces éléments doivent fixer D et a et sont des bi-3-cycles, les supports de leurs facteurs sont alors D et $\mathscr{S} \setminus (D \cup \{a\})$, mais cela ne permettant de contruire que 4 bi-3-cycles, c'est qu'il est impossible que $card(I) = 12$. De plus, I ne peut pas être trivial, sinon G contiendrait au moins 24^2 éléments, on en déduit alors qu'il s'agit du normalisateur d'un 3-Sylow.

Deuxième cas : si $a \in \mathscr{D}$. Notons D^1 et D^2 les uniques éléments de $\mathscr{D} \setminus \{D\}$ qui contiennent a. Puisque a et D sont stables sous l'action de I, on en déduit que la partition en orbites de $\mathscr{D}$ sous cette même action est plus fine que :

$$\mathscr{D} = \{D\} \cup \{D^1\,;\,D^2\} \cup \mathscr{D} \setminus \{D\,;\,D^1\,;\,D^2\}$$

Puisque les éléments d'ordre 3 sont des bi-3-cycles, cela suffit à montrer qu'il n'en existe pas dans I. Donc $card(I) \in \{1\,;\,2\,;\,4\,;\,8\}$. Il nous suffit maintenant d'exhiber, dans I, un élément d'ordre 4 et un élément d'ordre 2 qui ne commutent pas, pour obtenir que I est un 2-Sylow de G. Par exemple et sans perte de généralité, avec $(a,D) = (a_1,D_1)$, il suffit de prendre : $(a_6\ a_7\ a_5\ a_4)(a_3\ a_2)$ qui induit $(D_2\ D_7\ D_5\ D_6)(D_3\ D_4)$ et $(a_6\ a_5)(a_3\ a_2)$ qui induit $(D_2\ D_7)(D_5\ D_6)$.

Lemme 4.1.2 :

L'application qui à un sous-groupe d'ordre 24 de G associe l'unique sous-groupe de Klein distingué qu'il contient, est bijective de l'ensemble des sous-groupes d'ordre 24 dans l'ensemble des sous-groupes de Klein.

Preuve : Puisque l'on sait maintenant qu'un tel sous-groupe est isomorphe à $\mathfrak{S}_4$, il suffit de remarquer qu'il existe bien un unique sous-groupe d'ordre 4 et distingué dans $\mathfrak{S}_4$ (sous-groupe des bitranspositions et du neutre). De plus, si Γ et Γ' ont la même image, K, par cette application, alors ils sont tous les deux contenus dans le normalisateur de K dans G, or on a vu que l'orbite de K sous l'action par conjugaison de G sur ses sous-groupes est de cardinal 7 (lemme 3.1.1), on en déduit donc que le normalisateur de K est de cardinal 24, par suite, $\Gamma = \Gamma' = N_G(H)$. D'où l'injectivité de cette application. Reste maintenant à remarquer qu'il y a autant de sous-groupes de Klein que de sous-groupes d'ordre 24, ce qui donne la bijectivité. En effet, par le lemme précédant, on a que les stabilisateurs d'éléments de $\mathscr{S}$ ou de $\mathscr{D}$ sont tous distincts. Or $card(\mathscr{S}) = card(\mathscr{D}) = 7$, et l'on sait déjà qu'il existe 14 sous-groupes de Klein.

Propriété 4.1.5 :

Les sous-groupes d'ordre 12 de G sont exactement les sous-groupes isomorphes à $\mathfrak{A}_4$ des stabilisateurs d'élements de $\mathscr{S}$ ou $\mathscr{D}$.

Preuve : Soit H un sous-groupe d'ordre 12 de G. Puisqu'il s'agit d'un sous-groupe de G et qu'il est de cardinal 12, on a alors que les ordres de ses éléments sont 1, 2, 3 ou 4, ce qui nous donne aussi le fait que pour compter

ses éléments il suffit de compter ceux qui interviennent dans ses sous-groupes de Sylow. En outre, par le même raisonnement que dans la preuve du point (iii) du lemme 4.1.1, on a que H possède 4 3-Sylow. Par cardinalité, et par notre remarque, on en déduit alors qu'il existe un unique sous-groupe de Sylow pour le facteur 2. De fait, il est disintgué dans H. Par le lemme précédant, on en déduit alors que, si ce sous-groupe est un sous-groupe de Klein, alors H est inclu dans son normalisateur qui est un stabilisteur d'un élément de $\mathscr{S}$ ou $\mathscr{D}$ (on sait qu'il est distingué dans un tel sous-groupe, et il s'agit forcément de son normalisateur car il est de cardinal un diviseur strict maximal de 168 et que G est simple). H pouvant alors être identifier à un sous-groupe d'indice 2 dans $\mathfrak{S}_4$, on en déduit le résultat. S'il ne s'agit pas d'un sous-groupe de Klein, c'est un sous-groupe cyclique d'ordre 4, il est inclu dans un 2-Sylow qui est son normalisateur. En effet, puisque $\mathscr{O}_4$ est une classe de conjugaison de G, on en déduit que l'orbite d'un sous-groupe cyclique d'ordre 4 sous l'action par conjugaison de G est de cardinal 21, donc son normalisateur est de cardinal 8. Ce qui nous mène à une contradiction car on devrait avoir H inclu dans ce normalisateur, ce qui est impossible par cardinalité. On en déduit donc la propriété.

Propriété 4.1.6 :

G possède exactement 177 sous-groupes propres, qui sont d'ordre : 2, 3, 4, 6, 7, 8, 12, 21 ou 24.

Preuve : On sait déjà que les seuls ordres possibles des sous-groupes propres de G sont 2, 3, 4, 6, 7, 8, 12, 21 et 24, il nous suffit alors de les compter :
- Les sous-groupes d'ordre 2 sont ceux engendrés par les éléments d'ordre 2 ; or, on sait par la propriété 2.4.3 qu'il en existe 21.
- Les sous-groupes d'ordre 3 sont les 3-Sylow, et l'on en a dénombrés 28.
- Les sous-groupes d'ordre 4 sont soit les sous-groupes de Klein, dont on sait qu'ils sont au nombre de 14, soit les sous-groupes engendrés par des éléments d'ordre 4, il suffit, dans ce dernier cas, de remarquer que ces éléments vont deux par deux : eux-mêmes et leur inverse engendrent le même sous-groupe, ce qui fait alors 21 sous-groupes de ce type.
- Les sous-groupes d'ordre 6 étant exactement les normalisateurs des 3-Sylow, et puisqu'il ne peuvent contenir qu'un seul sous-groupe d'ordre 3, on en déduit qu'il en existe autant que de 3-sylow, c'est-à-dire 28.
- Les sous-groupes d'ordre 7 sont les 7-Sylow, on en a compté 8.
- Les sous-groupes d'ordre 8 sont les 2-Sylow, il en existe 21.
- Les sous-groupes d'ordre 12, par la propriété 4.1.5, sont en bijection avec les sous-groupes d'ordre 24.
- Les sous-groupes d'ordre 21 sont les normalisateurs des 7-Sylow de G, on sait aussi, puisqu'ils sont d'ordre 21, qu'ils ne contiennent qu'un seul sous-groupe d'ordre 7, donc il y en autant que de 7-Sylow, c'est-à-dire 8.
- Les sous-groupes d'ordre 24 étant les stabilisateurs des éléments de $\mathscr{S}$ ou de $\mathscr{D}$, on a vu qu'il en existe 14.
On en compte alors bien 177 au total.

Propriété 4.1.7 :

Les sous-groupes maximaux de G sont ses sous-groupes d'ordre 21 et 24.

Preuve : En ce qui concerne les sous-groupes d'ordre 21 ou 24, il suffit de voir, par la liste des cardinaux possibles des sous-groupes de G que l'on a établie, qu'il n'en existe pas étant divisible par 21 ou 24, inférieur strictement à 168 et strictement supérieur à 21 ou 24. Montrons alors que les autres sous-groupes ne sont pas maximaux.
Dans le cas de sous-groupes d'ordre 2 ou 4, le deuxième théorème de Sylow nous donne qu'ils sont inclus dans les 2-Sylow de G. Pour les sous-groupes d'ordre 3 ou 7, il suffit de remarquer qu'ils sont inclus dans leur normalisateur qui n'est pas G. Le cas des sous-groupes d'ordre 12 résulte de la propriété 4.1.5.
Étudions le cas des sous-groupes d'ordre 8. On sait qu'il s'agit des 2-Sylow de G. Soit $H \in \mathscr{S}_2$, et Γ un sous-groupe d'ordre 24. On sait qu'il existe : $K \in \mathscr{S}_2$ tel que $K \subset \Gamma$. Mais, rappelons que les 2-Sylow de G sont tous conjugués, d'après le deuxième théorème de Sylow. D'où, il existe $g \in G$ tel que $gKg^{-1} = H$. On en déduit alors que $H \subset g\Gamma g^{-1}$, qui est un sous-groupe d'ordre 24, la conjugaison par un élément de G étant un automorphisme.

Il nous reste alors à traiter le cas des sous-groupes d'ordre 6. On sait qu'il s'agit des normalisateurs des 3-Sylow de G. Soit H un sous-groupe d'ordre 6, normalisateur de $I \in \mathscr{S}_3$, et Γ un sous-groupe d'ordre 24. Remarquons qu'un 3-Sylow de Γ est un 3-Sylow de G et que le normalisateur dans Γ d'un 3-Sylow est de cardinal 6, il est donc aussi le normalisateur dans G dudit 3-Sylow. Soit alors K un normalisateur d'un 3-Sylow, J, de Γ. Montrons que H et K sont conjugués. Puisque les 3-Sylow de G sont tous conjugués, il existe $g \in G$ tel que $gJg^{-1} = I$. Mais puisque la conjugaison est un automorphisme, on a que $I = gJg^{-1}$ est distingué dans gKg^{-1}, on en déduit donc que $gKg^{-1} = H$. Par suite, $H \subset g\Gamma g^{-1}$, qui est un sous-groupe d'ordre 24.

4.2 Action par conjugaison de G sur ses sous-groupes

Le deuxième théorème de Sylow nous donne que G agit transitivement par conjugaison sur ses sous-groupes de Sylow. Mais qu'en est-il sur ses autres sous-groupes ? Une partie de la réponse est déjà prouvée, en effet, par ce que l'on a fait, on sait que les normalisateurs d'un certain type de sous-groupes de Sylow de G sont conjugués deux à deux sous l'action de G du fait qu'ils contiennent chacun un unique sous-groupe de Sylow. En outre, on a déjà étudié le cas des sous-groupes de Klein qui forment deux orbites sous cette action. De plus, en ce qui concerne les sous-groupes d'ordre 2 et les sous-groupes d'ordre 4 et cycliques de G, puisque les éléments d'ordre 2 et ceux d'ordre 4 forment chacun une classe de conjugaison, on sait alors qu'ils forment deux orbites sous l'action par conjugaison de G sur ses sous-groupes. Il ne nous reste alors qu'à prouver le résultat suivant :

Propriété 4.2.1 :

Sous l'action par conjugaison de G sur ses sous-groupes, l'ensemble des sous-groupes d'ordre 24 de G forme une union de deux orbites de cardinal 7.

Preuve : Rappelons que les sous-groupes d'ordre 24 de G sont exactement les stabilisateurs des éléments de $\mathscr{S}$ ou de $\mathscr{D}$. Puisque l'on sait que l'action de G sur $\mathscr{S}$ (resp. $\mathscr{D}$) est transitive, et puisque le conjugué par $g \in G$ d'un stabilisateur G_a (resp. G_D) d'un élément $a \in \mathscr{S}$ (resp. $D \in \mathscr{D}$) est le stabilisateur de $g.a \in \mathscr{S}$ (resp. $g.D \in \mathscr{D}$), on a déjà que tous les stabilisateurs d'éléments de $\mathscr{S}$ (resp. $\mathscr{D}$) sont conjugués, ce qui nous fait soit deux orbites de cardinal 7, soit une orbite de cardinal 14.
Supposons qu'il existe $g \in G$, $a \in \mathscr{S}$ et $D \in \mathscr{D}$ tels que : $gG_ag^{-1} = G_D$. Notons $b = g.a$. Par ce qui précède, on déduit que $G_b = G_D$. Cela signifie qu'un élément qui stabilise D fixe forcément b et inversement. Il suffit alors d'exhiber des éléments de G bien choisis afin d'obtenir le résultat attendu. Si $b \in D$, il suffit de prendre n'importe quel élément d'ordre 3 dans G_D, sinon, si $b \notin D$, on prend un élément d'ordre 4 dans G_D (dans les deux cas, ce sont pour des raisons de supports que ce sont des raisons suffisantes). On en déduit alors :

Propriété 4.2.2 :

Sous l'action par conjugaison de G sur ses sous-groupes, l'ensemble des sous-groupes d'ordre 12 de G forme une union de deux orbites de cardinal 7.

Preuve : Il suffit d'utiliser le lemme 4.1.1 et la propriété 4.2.1, en se rappelant qu'un sous-groupe d'ordre 24 de G possède un unique sous-groupe d'ordre 12, de par la propriété 4.1.5.

5 Les automorphismes de G

5.1 Le sous-groupe des automorphismes intérieurs de G

Définition et notations : (i) On définit les automorphismes intérieurs de G comme les morphismes qui correspondent à l'action d'un élément de G par conjugaison sur G. On vérifie de manière aisée qu'il s'agit alors bien d'un sous-groupe des automorphismes de G et qu'il est isomorphe à G (car $Z(G) = \{e_G\}$). On notera le sous-groupe des automorphismes intérieurs de G : $I(G)$, et le groupe des automorphismes : $Aut(G)$.

(ii) Pour des raisons qui deviendront claires, on introduit les notations $\mathscr{T}_1$, respectivement $\mathscr{T}_2$, afin de parler de l'orbite que forment les stabilisateurs d'éléments de $\mathscr{S}$, respectivement $\mathscr{D}$, sous l'action par conjugaison de G sur ses sous-groupes.

Propriété 5.1.1 :

$Aut(G)$ agit sur $\{\mathscr{T}_1;\mathscr{T}_2\}$ et le noyau de cette action est $I(G)$.

Preuve : Soit $\sigma \in Aut(G)$ et $H \in \mathscr{T}_1 \cup \mathscr{T}_2$. Puisque σ est un automorphisme $\sigma(H)$ est un sous-groupe d'ordre 24. De plus, si H est conjugué à un sous-groupe K par $g \in G$, on a que $\sigma(H)$ est conjugué à $\sigma(K)$ par $\sigma(g) \in G$. Donc $Aut(G)$ agit sur $\{\mathscr{T}_1;\mathscr{T}_2\}$.
Le fait qu'un automorphisme intérieur laisse $\mathscr{T}_1$ et $\mathscr{T}_2$ stables est évident par les définitions de $\mathscr{T}_1$ et $\mathscr{T}_2$, prouvons la réciproque. Soit $\phi \in Aut(G)$ tel que $\phi(\mathscr{T}_1) = \mathscr{T}_1$ et $\phi(\mathscr{T}_2) = \mathscr{T}_2$. Introduisons $\Gamma : a \in \mathscr{S} \longmapsto G_a$, le stabilisateur sous G de a. On vérifie aisément que Γ est une bijection. Soit aussi $\psi : a \in \mathscr{S} \longmapsto \Gamma^{-1} \circ \phi \circ \Gamma(a) \in \mathscr{S}$. Montrons qu'en fait $\psi \in G$. En effet, dire qu'il s'agit d'un élément de G c'est exactement dire qu'il s'agit d'une bijection de $\mathscr{S}$ et qu'il induit une bijection sur $\mathscr{D}$; or on a déjà la bijectivité sur $\mathscr{S}$, de par les définitions, enfin, le fait que ψ induise une bijection sur $\mathscr{D}$ découle du lemme suivant et d'un petit calcul :

Lemme 5.1.1 :

Tout triplet d'élément de $\mathscr{S}$, $\{a^1\,;a^2\,;a^3\}$, forme un élément de $\mathscr{D}$ si et seulement si $\left(\bigcap_{i=1}^{3} G_{a^i}\right) \in \mathscr{K}$.

Preuve : - Sens direct : reprenons le triplet de l'énoncé et supposons qu'il constitue un élément D de $\mathscr{D}$. On a alors que :

$$\bigcap_{i=1}^{3} G_{a^i} = \bigcap_{i=1}^{3} (G_{a^i} \cap G_D)$$

Or, par le lemme 4.1.1, on en déduit qu'il s'agit de l'intersection de trois 2-Sylow de G_D (et aussi de G). En outre, il sont distincts, par exemple et sans perte de généralité, pour $G_{a^1} \cap G_D$, on sait qu'il existe un élément d'ordre 4 et qu'il a un support de cardinal 6 (propriété 3.2.1.(i)), il n'appartient donc pas à $G_{a^2} \cup G_{a^3}$. Et puisque $G_D \simeq \mathfrak{S}_4$, il s'agit d'un sous-groupe de Klein (sous-groupe des bitranspositions et du neutre).
- Sens réciproque : Supposons que l'on a bien $\left(\bigcap_{i=1}^{3} G_{a^i}\right) \in \mathscr{K}$ mais que $\{a^1\,;a^2\,;a^3\} \notin \mathscr{D}$. Notons D l'unique élément de $\mathscr{D}$ tel que $\{a^1\,;a^2\} \subset D$. On a évidemment :

$$\left(\bigcap_{i=1}^{3} G_{a^i}\right) \subset (G_D \cap G_{a^3})$$

Or, cette dernière intersection est isomorphe à $\mathfrak{S}_3$ (lemme 4.1.1), donc elle ne peut pas contenir de sous-groupe de Klein, ce qui est une contradiction à nos hypothèses. De fait $\{a^1\,;a^2\,;a^3\} \in \mathscr{D}$.

Revenons à la preuve de la propriété, rappelons que l'on veut montrer que ψ induit une bijection sur $\mathscr{D}$. Soit un élément de $\mathscr{D}$: $\{a^1\,;a^2\,;a^3\}$, observons l'intersection des stabilisateurs des éléments du triplet : $\{\psi(a^1)\,;\psi(a^2)\,;\psi(a^3)\}$. Remarquons d'abords que :

$$\begin{aligned} G_{\psi(a^i)} &= G_{\Gamma^{-1}\circ\phi(G_{a^i})} \\ &= G_{\Gamma^{-1}(G_{b^i})} && \text{où } b^i \in \mathscr{S} \text{ tel que } G_{b^i} = \phi(G_{a^i}) \\ &= G_{b^i} = \phi(G_{a^i}) \end{aligned}$$

Dont on déduit :

$$\bigcap_{i=1}^{3} G_{\psi(a^i)} = \bigcap_{i=1}^{3} \phi(G_{a^i}) = \phi\left(\bigcap_{i=1}^{3} G_{a^i}\right) \in \mathscr{K} \text{ (car } \phi \text{ est un automorphisme)}$$

On en conclut donc bien que ψ induit alors une bijection sur $\mathscr{D}$, et de fait $\psi \in G$.
Montrons maintenant que ϕ correspond à l'automorphisme intérieur construit à partir de ψ, c'est-à-dire :

$$\overline{\psi} \ : \ g \ \in \ G \longmapsto \ \psi \, g \, \psi^{-1} \ \in \ G$$

Par le calcul effectué plus haut, on sait que $\overline{\psi}$ et ϕ induisent la même action sur les stabilisateurs d'éléments de $\mathscr{S}$. Montrons alors que $\overline{\psi}$ et ϕ induisent la même action sur les stabilisateurs d'éléments de $\mathscr{D}$ aussi, ce dont on déduira qu'ils coïncident sur les éléments d'ordre 2. Ensuite il nous suffira de montrer que les éléments d'ordre 2 engendrent G, ce qui nous donnera le résultat.
Soit $D = \{a^1 ; a^2 ; a^3\} \in \mathscr{D}$, on a :

$$\begin{aligned}
\psi(D) &= \bigcup_{i=1}^{3} \{\psi(a^i)\} && \text{définition de l'action induite par } \psi \text{ sur } \mathscr{D} \\
&= \bigcup_{i=1}^{3} \{\Gamma^{-1} \circ \phi \circ \Gamma(a^i)\} = \bigcup_{i=1}^{3} \{\Gamma^{-1} \circ \phi(G_{a^i})\} \\
&= \bigcup_{i=1}^{3} \{\alpha^i\} && \text{où } \alpha^i \text{ est tel que } G_{\alpha^i} = \phi(G_{a^i})
\end{aligned}$$

Posons maintenant $V \in \mathscr{D}$ tel que $G_V = \phi(G_D)$. Par le lemme 4.1.1, on a que pour $i \in \{1;2;3\}$: $(G_D \cap G_{a^i})$ est un 2-Sylow. Puisque ϕ est un automorphisme, on en déduit que pour $i \in \{1;2;3\}$: $(G_v \cap G_{\alpha^i}) \in \mathscr{S}_2$. Toujours par le lemme 4.1.1, on en déduit $V = \{\alpha^1;\alpha^2;\alpha^3\}$. D'où :

$$\overline{\psi}(G_D) = \psi G_D \psi^{-1} = G_{\psi(D)} = G_V = \phi(G_D)$$

Par la bijection du lemme 4.1.2, et le fait que l'image d'un sous-groupe distingué par un automorphisme est encore un sous-groupe distingué, on obtient que $\overline{\psi}$ et ϕ induisent la même action sur $\mathscr{K}$. Soit alors $x \in \mathscr{O}_2$, on a déjà remarqué que $Z(x) \in \mathscr{S}_2$, or puisqu'il est isomorphe à D_8 (propriété 2.4.4), on sait qu'il contient 2 sous-groupes de Klein, K_1 et K_2, qui s'intersectent en son centre qui est $\{e_G;x\}$. Puisque $\overline{\psi}(K_1) = \phi(K_1)$ et $\overline{\psi}(K_2) = \phi(K_2)$, on a $\overline{\psi}(< x >) = \phi(< x >)$, et puisqu'il s'agit d'automorphismes, on a en fait : $\overline{\psi}(x) = \phi(x)$. Reste à voir que les éléments d'ordre 2 engendrent G. Par les propriétés du groupe diédral à 8 éléments, on sait que les éléments d'ordre 2 engendrent les éléments d'ordre 4, autrement dit : $\{e_G\} \sqcup \mathscr{O}_2 \sqcup \mathscr{O}_4 \subset < \mathscr{O}_2 >$, donc $< \mathscr{O}_2 >$ est un sous-groupe de G de cardinal supérieur à 64, on en déduit bien que les éléments d'ordre 2 engendrent G.

Propriété 5.1.2 :

$I(G)$ est d'indice 2 dans $Aut(G)$.

Preuve : De par la propriété 5.1.1, on sait que l'on dispose d'un morphisme $\rho : Aut(G) \to \mathfrak{S}_{\{\mathscr{T}_1;\mathscr{T}_2\}} \simeq \mathbb{Z}/2\mathbb{Z}$ et que $Ker(\rho) = I(G)$, il suffit alors de remarquer que ρ est surjectif et d'utiliser la factorisation canonique. Si l'on considère G en tant que $GL_3(\mathbb{F}_2)$, il suffit de remarquer que l'application $M \to {}^tM^{-1}$ est un automorphisme de G qui échange $\mathscr{T}_1$ et $\mathscr{T}_2$. En effet, si M est un élément qui fixe une droite de $\mathbb{F}_2^3$ alors ${}^tM$ fixe le plan qui lui est orthogonal et prendre l'inverse n'y change rien. Il s'agit alors de l'élément qui envoie $\mathscr{T}_1$ sur $\mathscr{T}_2$, et inversement puisque l'on est dans $\mathfrak{S}_{\{\mathscr{T}_1;\mathscr{T}_2\}}$.

5.2 Le groupe des automorphismes de G

Afin de faire des calculs explicites, nous utiliserons ici l'identification de G au groupe $PSL_2(\mathbb{F}_7)$, mais vérifions d'abord que cela est possible. Puis nous déterminerons la structure du groupe des automorphismes.

Propriété 5.2.1 :

Le groupe $PSL_2(\mathbb{F}_7)$ est non abélien, de cardinal 168 et simple, par le théorème d'unicité d'un tel groupe, il est donc isomorphe à G.

Preuve : Comptons d'abord son nombre d'éléments. Ici, contrairement au cas de $PSL_3(\mathbb{F}_2)$, nous n'avons pas d'identification avec le groupe linéaire, déroulons donc la définition, commençons par le cardinal de $GL_2(\mathbb{F}_7)$. Pour ce dernier, compter le nombre d'éléments revient à compter le nombre de bases dans $\mathbb{F}_7^2$. Pour construire une base, on dispose alors de 7^2-1 choix pour le premier vecteur - le vecteur nul étant écarté - puis de 7^2-7 autres pour le second vecteur - le nul et les vecteurs colinéaires au premier étant exclus. Ce qui fait alors 2016 éléments. En outre, par la factorisation du déterminant, on en déduit que $card(SL_2(\mathbb{F}_7)) = 336$, car $card(\mathbb{F}_7^\times) = 6$. Il nous suffit maintenant de remarquer que $Z(SL_2(\mathbb{F}_7)) = \{I\,;\,-I\}$, ce qui nous conduit à $card(PSL_2(\mathbb{F}_7)) = 168$. La preuve de la simplicité peut se faire par adaptation de la preuve déjà effectuée pour $PSL_3(\mathbb{F}_2)$.

Théorème 5.2.1 :

$$Aut(G) \simeq PGL_2(\mathbb{F}_7)$$

Preuve : On utilise ici le plongement naturel de $PSL_2(\mathbb{F}_7)$ dans $PGL_2(\mathbb{F}_7)$. Considérons le morphisme suivant :

$$\Psi : \begin{cases} PGL_2(\mathbb{F}_7) \longrightarrow Aut(G) \\ \alpha \longmapsto \Psi(\alpha) : \begin{cases} G \longrightarrow G \\ s \longmapsto \alpha s \alpha^{-1} \end{cases} \end{cases}$$

On vérifie facilement qu'il s'agit d'un morphisme. Montrons qu'il est injectif : soit $\alpha \in PGL_2(\mathbb{F}_7)$ tel que :

$$\forall s \in G : \Psi(\alpha)(s) = s$$

On en déduit alors que $\Psi(\alpha)$ est un morphisme qui n'échange pas $\mathscr{T}_1$ et $\mathscr{T}_2$, donc il s'agit d'un morphisme intérieur (propriété 5.1.1). Par cette relation, on a même $\alpha \in Z(PSL_2(\mathbb{F}_7))$. Or ce groupe est trivial, d'où l'injectivité de Ψ. Remarquons maintenant que $PGL_2(\mathbb{F}_7)$ et $Aut(G)$ sont de cardinal 336, en effet, il y a clairement bijection entre G et $I(G)$, et puisque l'on sait que $[Aut(G) : I(G)] = 2$, on en déduit le cardinal de $Aut(G)$. Pour calculer le cardinal de $PGL_2(\mathbb{F}_7)$, il suffit de revenir à sa définition, pour cela, on a déjà montré que $card(GL_2(\mathbb{F}_7)) = 2016$ et on a $card(\mathbb{F}_7^\times) = 6$, d'où ces égalités. On en déduit alors que Ψ est un isomorphisme, d'où le théorème.

6 La table des caractères de G

Dans cette partie nous allons déterminer la table des caractères des représentations linéaires irréductibles complexes du groupe G. Notons que l'on utilise allègrement sans le rappeler, le fait que pour une représentation ρ et $g \in G$, $\rho(g)$ diagonalise dans une certaine base car est annulé par le polynôme à racines simples : $X^{168}-1$.

Propriété 6.1 :

G possède 6 représentations irréductibles à isomorphisme près.

Preuve : On sait déjà que G possède 6 classes de conjugaison, d'où le résultat.

Lemme 6.1 :

Si (ρ, V) est une représentation irréductible et non triviale de G, alors ρ est injective et pour tout $g \in G$:
$$det(\rho(g)) = 1.$$

Preuve : L'injectivité n'est que le résultat de la simplicité de G et du fait que ρ est une représentation irréductible et non triviale. De plus, si $det(\rho(g)) \neq 1$, pour un g fixé, on en déduit alors, en identifiant G à son image, que $\{I\} \subsetneq G \cap SL(V) \subsetneq G$, alors que $G \cap SL(V)$ est distingué dans G, ce qui ne se peut.

Propriété 6.2 :

G ne possède pas de représentation irréductible complexe de dimension 2.

Preuve : Procédons par l'absurde, supposons que l'on dispose d'une représentation irréductible :

$$\rho : G \longrightarrow GL(V) \simeq GL_2(\mathbb{C})$$

On sait que ρ est injective, par le lemme 6.1, donc, pour $x \in \mathscr{O}_2$, on a $ord(\rho(x)) = 2$, et puisque $\rho(G) \simeq G$, on en déduit que $\rho(x)$ ne peut pas être un élément central (car le centre est trivial dans *G*), donc à conjugaison près :

$$\rho(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Dans ce cas, $det(\rho(x)) = -1$. Une telle représentation ne peut alors pas exister.

Propriété 6.3 :

La liste des dimensions des représentations irréductibles de *G* à isomorphisme près est : 1, 3, 3, 6, 7, 8.

Preuve : On sait qu'il existe $[G : D(G)]$ représentations irréductibles de dimension 1, or *G* étant non abélien et simple, il n'existe alors que la représentation unité, de ce type. Pour le reste, il suffit d'utiliser les faits suivants : pour *V* une représentation irréductible de *G*, $dim(V) \mid card(G)$ et que si l'ensemble des représentations irréductibles distinctes à isomorphisme près est $\{V_1 ; V_2 ; V_3 ; V_4 ; V_5 ; V_6\}$, on a $\sum_{i \in [\![1;6]\!]} dim(V_i)^2 = card(G)$. Et alors, la seule liste possible est celle énoncée.

Lemme 6.2 :

Un élément d'ordre 7 n'est jamais conjugué à son inverse.

Preuve : Procédons par l'absurde, soit $g \in \mathscr{O}_7$ tel qu'il existe $x \in G$ tel que $xgx^{-1} = g^{-1}$. En partant de *g* et de g^{-1} et en utilisant le fait que tous les 7-Sylow de *G* sont conjugués, on obtient alors déjà 16 éléments de la classes de conjugaison de *g*, que l'on notera : $cl(g)$. Or on sait que $card(cl(g)) = 24$ (propriété 2.5.1). Soit alors $p \in cl(g)$ distincts de tous ceux déjà trouvés. Grâce au fait que tous les 7-Sylow sont conjugués, on peut supposer que $p \in < g > \in \mathscr{S}_7$, de fait, il existe $k \in [\![2;6]\!] \setminus \{-1\}$ tel que $p = g^k$. Mais alors, puisque $xgx^{-1} = g^{-1}$, on en déduit $xg^kx^{-1} = g^{-k} = p^{-1}$. Puis, en partant de *p* et p^{-1}, et du fait que les 7-Sylow sont conjugués, on dénombre encore 16 éléments de $cl(g)$ (distincts de ceux déjà trouvés), ce qui est trop. Par l'absurde, on a donc que *g* n'est pas conjugué à g^{-1}.

Propriété 6.4 :

Les colonnes de $\mathscr{C}_1$ et $\mathscr{C}_2$ sont conjugués.

Preuve : Conséquence immédiate du lemme précédent et du fait qu'il n'existe que deux classes de conjugaison formées par des éléments d'ordre 7.

Propriété 6.5 :

Il n'existe qu'un seul complexe et son conjugué dans la table des caractères de *G* qui ne sont pas réels. Ils se situent sur les lignes correspondant aux représentations de dimension 3 et sur les colonnes de $\mathscr{C}_1$ et de $\mathscr{C}_2$.

Preuve : Remarquons que puisqu'il n'existe qu'une représentation de dimension 1, 6, 7 ou 8, on en déduit que les représentations de de dimension 1, 6, 7 ou 8 sont auto-duales et, de fait, il n'existe pas de complexe non réel sur leur ligne de caractères, car la ligne de la duale est la conjuguée. Or, puisque deux colonnes de deux classes de conjugaison disctinctes ne peuvent être égales et que la colonne de $\mathscr{C}_1$ et de $\mathscr{C}_2$ sont conjugués l'une de l'autre, on en déduit qu'il existe un complexe non réel sur chacune d'entre elles et qu'il est forcément sur la ligne des caractères d'une représentation de dimension 3. De plus, les autres classes de conjugaison étant l'ensemble des éléments d'un ordre donné, on en déduit qu'elles ne comportent aucun complexe non réel, d'où la propriété.

Remarque : Cela nous donne aussi que les deux représentations de dimension 3 sont duales l'une de l'autre.

Propriété 6.6 :

Si (ρ, V) est une représentation irréductible de dimension 3 de G et si χ est son caractère, alors : $\chi(\mathscr{O}_2) = -1$, $\chi(\mathscr{O}_3) = 0$, $\chi(\mathscr{O}_4) = 1$

Preuve : $\chi(\mathscr{O}_2)$:
Si $x \in \mathscr{O}_2$, puisque l'on sait que ρ est injectif, $ord(\rho(x)) = 2$. En écartant toujours le cas d'un élément central, on en déduit alors que, à conjugaison près :

$$\rho(x) \in \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} ; \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\}$$

Mais rappelons que $det(\rho(x)) = 1$, donc la seule possibilité est la première, et on obtient $\chi(\mathscr{O}_2) = -1$.

$\chi(\mathscr{O}_3)$:
Soit $t \in \mathscr{O}_3$, on a $ord(\rho(t)) = 3$, donc soit j soit j^2 est dans le spectre de $\rho(t)$, mais puisque $\chi(\rho(t)) \in \mathbb{R}$, on en déduit que les valeurs propres de $\rho(t)$ sont exactement les racines troisièmes de l'unité, et, de fait, $\chi(\mathscr{O}_3) = 0$.

$\chi(\mathscr{O}_4)$:
Soit $y \in \mathscr{O}_4$. On a, à conjugaison près, $\rho(y)^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, de fait, $\rho(y) = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm i & 0 \\ 0 & 0 & \pm i \end{pmatrix}$. Mais puisque $tr(\rho(y)) \in \mathbb{R}$, alors, à conjugaison près, $\rho(y) = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & i \end{pmatrix}$, et enfin, avec $det(\rho(y)) = 1$, on en déduit : $\rho(y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & i \end{pmatrix}$. De fait $\chi(\mathscr{O}_4) = 1$.

Propriété 6.7 :

Les trois premières lignes sont :

	1	21	56	42	24	24
	$\mathscr{O}_1$	$\mathscr{O}_2$	$\mathscr{O}_3$	$\mathscr{O}_4$	$\mathscr{C}_1$	$\mathscr{C}_2$
U	1	1	1	1	1	1
V_1	3	-1	0	1	$\frac{1}{2}(-1+i\sqrt{7})$	$\frac{1}{2}(-1-i\sqrt{7})$
V_2	3	-1	0	1	$\frac{1}{2}(-1-i\sqrt{7})$	$\frac{1}{2}(-1+i\sqrt{7})$

Preuve : Sur ces lignes, il ne nous manque que le complexe non réel et son conjugué, dont on trouve la partie réelle en utilisant l'orthogonalité de la ligne de V_1 avec la ligne de U, et dont on déduit la partie imaginaire avec le fait que la somme des carrés des modules des élément de la ligne V_1 est 1.

Propriété 6.8 :

Si (ρ, V) est une représentation irréductible de dimension 7 de G et χ est son caractère, alors
$$\chi(\mathscr{C}_1) = \chi(\mathscr{C}_2) = 0.$$

Preuve : Soit $x \in \mathscr{O}_7$. On sait que x et x^{-1} ne sont pas conjugués, on sait aussi qu'il existe un $y \in < x > \cap cl(x)$ [4]. Soit k tel que $y = x^k$. On en déduit alors que : pour $p \in \mathbb{Z}$, x et $x^{k^p[7]}$ sont conjugués. Or si $k \in \{3\,;5\,;6\}$, cela donnerait que x^{-1} est conjugué à x (il suffit de prendre un "bon" p). Et si x est conjugué à x^2 alors il l'est à x^4 et vice versa. On en déduit donc que $\{x^2\,;x^4\} \subset cl(x)$.
En notant $Sp(\rho(x))$ le spectre de $\rho(x)$, on sait qu'il existe ξ, racine septième primitive de l'unité, telle que $\xi \in Sp(\rho(x))$ (car $ord(\rho(x)) = 7$ puisque ρ est injectif), donc $\xi^2 \in Sp(\rho(x)^2)$ et $\xi^4 \in Sp(\rho(x)^4)$. Or, puisque $\{x^2\,;x^4\} \subset cl(x)$, on en déduit $\{\xi\,;\xi^2\,;\xi^4\} \in Sp(\rho(x))$. Mais, puisque $tr(\rho(x)) \in \mathbb{R}$ et que $Sp(\rho(x))$ est inclu dans l'ensemble des racines septièmes de l'unité, on a $\xi^{-1} \in Sp(\rho(x))$. Mais alors, par un raisonnement que l'on vient de faire, on en déduit que toutes les racines septièmes primitives de l'unité sont dans $Sp(\rho(x))$, et elle n'apparaissent qu'une seule fois et $Sp(\rho(x))$ est complété par 1 car $tr(\rho(x)) \in \mathbb{R}$. On en déduit la forme de $\rho(x)$ et $\chi(\mathscr{C}_1) = \chi(\mathscr{C}_2) = 0$.

Propriété 6.9 :

Si (ρ, V) est une représentation irréductible de dimension 6 de G et χ est son caractère, alors
$$\chi(\mathscr{C}_1) = \chi(\mathscr{C}_2) = -1.$$

Preuve : Par les même types d'arguments, pour $y \in \mathscr{O}_7$, on montre que $\rho(y)$ a pour valeurs propres, exactement les racines septièmes primitives de l'unité, d'où le résultat.

Propriété 6.10 :

Si (ρ, V) est une représentation irréductible de dimension 8 de G et χ est son caractère, alors
$$\chi(\mathscr{C}_1) = \chi(\mathscr{C}_2) = 1.$$

Preuve : Même preuve encore, mais ici il faut remarquer, en plus, que 1 appartient au spectre, et que, donc, ce dernier est formé des racines primitives septièmes de l'unité et de 1 avec multiplicité 2. D'où le résultat.

Théorème 6.1 :

La table des caractères de G est :

	1	21	56	42	24	24
	$\mathscr{O}_1$	$\mathscr{O}_2$	$\mathscr{O}_3$	$\mathscr{O}_4$	$\mathscr{C}_1$	$\mathscr{C}_2$
U	1	1	1	1	1	1
V_1	3	-1	0	1	$\frac{1}{2}(-1+i\sqrt{7})$	$\frac{1}{2}(-1-i\sqrt{7})$
V_2	3	-1	0	1	$\frac{1}{2}(-1-i\sqrt{7})$	$\frac{1}{2}(-1+i\sqrt{7})$
V_3	6	2	0	0	-1	-1
V_4	7	-1	1	-1	0	0
V_5	8	0	-1	0	1	1

4. En effet, en partant de x et en utilisant le théorème de Sylow, on dénombre déjà un conjugué à x dans chaque 7-Sylow. Puis, puisque $card(\mathscr{S}_7) = 8 < 24 = card(cl(x))$, on choisit $y \in cl(x)$, n'étant pas un de ceux déjà trouvés. Si $y \in < x >$, on a ce que l'on cherche, sinon, il existe $g \in G$ tel que $gxg^{-1} = y$, et $< y > \in \mathscr{S}_7$. On sait qu'il existe $k \in [\![2\,;6]\!]$tel qu'il existe $h \in G$ et $hxh^{-1} = y^k$ par suite : $x = h^{-1}gx^kg^{-1}h$, ce que l'on recherchait.

Preuve : On connaît déjà les trois premières lignes, la première colonne et les deux dernières. Si on note 1, -1, -1, x, y, z la colonne de $\mathscr{O}_2$, on pose alors le système :

$$\begin{cases} (\mathscr{O}_2, \mathscr{O}_1) = 0 & (1) \\ (\mathscr{O}_2, \mathscr{C}_1) = 0 & (2) \\ (\mathscr{O}_2, \mathscr{O}_2) = 168/21 & (3) \end{cases}$$

Or :

$$(2) \Leftrightarrow x = z + 2$$

Donc

$$(1) \Leftrightarrow y = -1 - 2z$$

Et par la propriété 6.5, on en déduit :

$$(3) \Leftrightarrow z(8 + 6z) = 0$$

Rappelons que, si $\mathscr{O}$ est l'ensemble des entiers algébirques, on a que $z \in \mathscr{O}$ et $\mathscr{O} \cap \mathbb{Q} = \mathbb{Z}$, de fait, $z = 0$ et on en déduit donc la colonne de $\mathscr{O}_2$.
En ce qui concerne les autres colonnes, il suffit de poser les systèmes :

$$\begin{cases} (\mathscr{O}_3, \mathscr{O}_1) = 0 \\ (\mathscr{O}_3, \mathscr{O}_2) = 0 \\ (\mathscr{O}_3, \mathscr{C}_1) = 0 \end{cases} \quad \text{et} \quad \begin{cases} (\mathscr{O}_4, \mathscr{O}_1) = 0 \\ (\mathscr{O}_4, \mathscr{O}_2) = 0 \\ (\mathscr{O}_4, \mathscr{O}_3) = 0 \end{cases}$$

Qui sont des systèmes linéaires à 3 inconnues, le reste de la colonne de $\mathscr{O}_3$ et de la colonne $\mathscr{O}_4$, respectivement, et à 3 équations indépendantes, ce dont on déduit alors le reste de la table.

7 Bibliographie

PERRIN Daniel, *Cours d'algèbre* (chapitre 5 partie 4 et exercices parties 4 et 5 du chapitre 5)
ARNAUDIÈS Jean-Marie, BERTIN José, *Groupes, algèbres et géométrie* (tome 1 chapitre 7 et exercices)