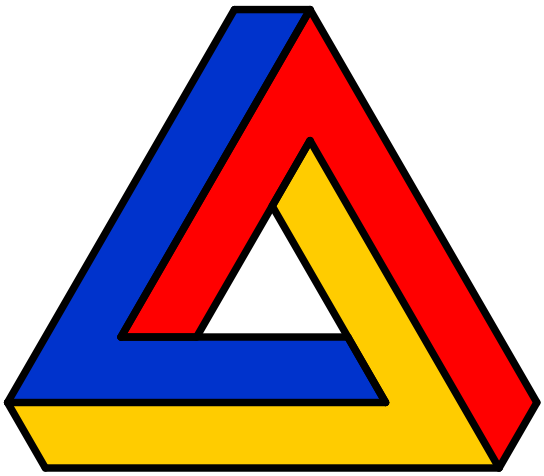
UNIVERSITÉ Grenoble Alpes

INSTITUT FOURIER

GROUPE SIMPLE D'ORDRE 168

Hubert Villuendas
Encadré par Grégory Berhuy



Master Mathématiques Générales
Année Universitaire 2021-2022

Table des matières

Introduction **2**

1 Existence d'un groupe simple d'ordre 168 **3**
1.1 Un coup d'œil au groupe linéaire $GL_3(\mathbb{F}_2)$ . . . 3
1.1.1 Classes de conjugaison . . . 3
1.1.2 Ordre des classes de conjugaison . . . 9
1.1.3 Simplicité de $GL_3(\mathbb{F}_2)$ . . . 11
1.2 Le groupe spécial projectif linéaire $PSL(E)$ . . . 12
1.2.1 Généralités sur le groupe spécial linéaire $SL(E)$ . . . 12
1.2.2 Simplicité du groupe spécial projectif linéaire $PSL(E)$ . . . 14
1.2.3 Le cas $PSL_2(\mathbb{F}_7)$ . . . 17
1.3 Un isomorphisme entre $GL_3(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_7)$? . . . 17
1.3.1 Espace projectif . . . 17
1.3.2 Étude fonctionnelle du groupe $GL_3(\mathbb{F}_2)$ . . . 19
1.3.3 Un portrait de $PSL_2(\mathbb{F}_7)$ . . . 21
1.3.4 L'isomorphisme $GL_3(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_7)$ . . . 22
1.4 Complément : autre point de vue sur $GL_3(\mathbb{F}_2)$ . . . 24

2 Unicité d'un groupe simple d'ordre 168 **25**
2.1 Quelques outils pour l'étude de la structure des groupes finis . . . 25
2.1.1 Les théorèmes de Sylow . . . 25
2.1.2 Indices de sous-groupes . . . 26
2.1.3 Action doublement transitive . . . 26
2.1.4 Lemme N/C . . . 27
2.2 Étude générale d'un groupe simple d'ordre 168 . . . 28
2.2.1 Les 7-Sylow de G . . . 28
2.2.2 Les 3-Sylow de G . . . 29
2.2.3 Les 2-Sylow de G . . . 31
2.3 Une première preuve par les homographies . . . 33
2.3.1 Un système de générateurs pour G . . . 33
2.3.2 Conditions d'appartenance à $PSL_2(k)$ . . . 36
2.3.3 L'unicité du groupe simple d'ordre 168 . . . 37
2.4 Plan de Fano . . . 37
2.4.1 Rappels sur $\mathfrak{S}_4$ et D_8 . . . 37
2.4.2 Groupes de Klein de G . . . 38
2.4.3 Relation entre les groupes de Klein de G . . . 41
2.4.4 Plan de Fano, ou $\mathbb{P}^2\left(\mathbb{F}_2\right)$ . . . 43

3 Table des caractères du groupe simple d'ordre 168 **46**
3.1 Représentation par permutation . . . 46
3.1.1 Définitions et résultats . . . 46
3.1.2 Représentation de degré 6 . . . 49
3.1.3 Représentation de degré 7 . . . 51
3.2 Représentation de degré 8 . . . 52
3.3 Représentations de degré 3 . . . 55
3.3.1 Anneau des entiers algébriques . . . 56
3.3.2 Calcul des caractères . . . 57
3.4 Table des caractères . . . 59

Références **60**

Introduction

À l'origine de la théorie des groupes, il y a sans doute la fâcheuse manie des mathématicien·ne·s de vouloir généraliser tous les concepts qui leur tombent sous la main. Les notions les plus élémentaires n'échappent pas à ce processus d'abstraction : pensons par exemple à l'addition sur les entiers. Nous pouvons noter qu'additionner consiste à combiner deux nombres pour en construire un troisième, et que cette opération a quelques propriétés particulières : l'existence d'un neutre 0, d'un inverse $-n$ pour tout entier n, et l'associativité qui nous permet de nous passer de parenthèses.

Que dire maintenant d'un ensemble muni d'une opération qui aurait ces mêmes propriétés ? C'est le résultat du processus d'abstraction d'opérations simples comme l'addition et la multiplication ; un tel ensemble doté d'une telle loi est appelé « groupe », et il est dit fini s'il ne contient qu'un nombre fini d'éléments.

Les groupes finis apparaissent alors naturellement un peu partout : ce sont eux qui régissent les symétries d'un flocon de neige, les mouvements possibles au Rubik's cube, ou encore les symétries des molécules. Ainsi comprendre les groupes, c'est comprendre ces objets.

La bonne notion pour comprendre la structure de ces groupes finis et celle de sous-groupe distingué : si $H \lhd G$, alors le quotient G/H admet une structure naturelle de groupe, dont l'étude peut nous donner de précieuses informations sur la structure de G. On remarque toutefois que construire un tel quotient n'a d'intérêt que si H est un sous-groupe propre de G. Mais alors que dire des groupes qui n'admettent pas de sous-groupes propres distingués ? De tels groupes sont dit « simples », et leur existence peuvent soulever quelques questions : y a-t-il des groupes simples d'ordre n, pour $n \in \mathbb{N}^*$? Pour un ordre donné, combien y a-t-il de groupes simples à isomorphisme près ?

Un des résultats les plus surprenants de la théorie des groupes est que les groupes simples ne peuvent avoir que quelques structures possibles : il est donc possible de les classer dans un nombre fini de familles. Là où les chimistes ont le tableau périodique des éléments, les algébristes ont la classification des groupes finis simples, et ainsi tout groupe simple G est, à isomorphisme près, soit :

- Un groupe cyclique d'ordre premier, $G \simeq \mathbb{Z}/p\mathbb{Z}$.
- Un groupe alterné, $G \simeq \mathfrak{A}_n$ avec $n \geqslant 5$.
- Un groupe classique, qui sont des sous-groupes ou des quotients de $\mathrm{GL}_n\left(\mathbb{F}_q\right)$, avec $q = p^m$, comme par exemple un groupe projectif spécial linéaire, ou un groupe orthogonal, *etc*.
- Un groupe de Lie.
- Un des vingt-six groupes sporadiques, c'est-à-dire les groupes qui ne peuvent pas être classés dans une des familles précédentes, et dont le plus grand groupe est le « groupe du Monstre » dont l'ordre est :

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

La démonstration de ce résultat, appelé *enormous theorem*, est un ensemble d'articles publiés pendant une durée de plus de vingt ans par plus d'une centaine d'auteurs, et compte plus de 10 000 pages.

Pourquoi s'intéresser à l'ordre 168 en particulier ? Regardons les deux premières familles de groupes simples. Les groupes cycliques et les groupes alternés sont des groupes que l'on connait relativement bien, et si l'on s'intéresse aux groupes simples d'ordre non premier, nous pouvons dire que le plus petit d'entre eux est d'ordre 60, et qu'il est isomorphe à $\mathfrak{A}_5$. Le suivant est un groupe simple d'ordre 168, et il est en fait unique à isomorphisme près.

Dans ce TER nous nous intéresserons à la preuve de l'existence et de l'unicité du groupe simple d'ordre 168, en voyant ce groupe tantôt comme $\mathrm{GL}_3(\mathbb{F}_2)$, tantôt comme un groupe projectif spécial linéaire ; et nous montrerons son unicité en déterminant quelques propriétés structurelles sur ses éléments et ses sous-groupes, ce qui nous permettra d'identifier G à $\mathrm{PSL}_2(\mathbb{F}_7)$ grâce aux homographies, ou encore en donnant une géométrie à certains ensembles de sous-groupes de G pour l'identifier au groupe d'automorphisme d'un certain plan projectif fini. Enfin, nous dresserons la table des caractères de G en essayant de construire les représentations du groupe simple d'ordre 168 à partir de son action sur différents ensembles.

1 Existence d'un groupe simple d'ordre 168

1.1 Un coup d'œil au groupe linéaire $\mathrm{GL}_3(\mathbb{F}_2)$

On s'intéresse ici au groupe spécial linéaire.

Proposition 1.1.1 (Cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$)**.** *Soit p premier et $n \in \mathbb{N}$. Alors :*

$$|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{k=1}^{n} \left(p^n - p^{k-1}\right)$$

Démonstration. Pour une base $(e_1, \cdots, e_n)$ de $\mathbb{F}_p^n$ fixée, un élément $\varphi \in \mathrm{GL}_n(\mathbb{F}_p)$ est entièrement déterminé par l'image de chaque vecteur de la base par φ, avec comme contrainte que la famille $\left(\varphi(e_1), \cdots, \varphi(e_n)\right)$ doit être une famille libre.
Le vecteur $\varphi(e_1)$ doit donc être un vecteur de $\mathbb{F}_p^n$ non nul, il y a donc $p^n - 1$ possibilités. Le vecteur e_2 quant à lui ne peut être envoyé sur aucun élément de $\mathrm{Vect}_{\mathbb{F}_p}\left(\varphi(e_1)\right)$, il reste donc $p^n - p$ possibilités pour $\varphi(e_2)$, et ainsi de suite.
Ainsi $\varphi(e_k)$ ne doit pas appartenir à $\mathrm{Vect}_{\mathbb{F}_p}\left(\varphi(e_1), \cdots, \varphi(e_{k-1})\right)$, il reste donc $p^n - p^{k-1}$ possibilités.
Finalement, on a bien :

$$|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{k=1}^{n} \left(p^n - p^{k-1}\right)$$

□

Dans le cas particulier où $p = 2$ et $n = 3$, on a :

$$|\mathrm{GL}_3(\mathbb{F}_2)| = \left(2^3 - 1\right)\left(2^3 - 2\right)\left(2^3 - 2^2\right) = 7 \cdot 6 \cdot 4 = 168$$

Ainsi $\mathrm{GL}_3(\mathbb{F}_2)$ est un groupe d'ordre 168, et on se propose de l'étudier pour montrer sa simplicité.

1.1.1 Classes de conjugaison

On peut désormais commencer à essayer de déterminer les classes conjugaison de $\mathrm{GL}_3(\mathbb{F}_2)$.
Pour cela, on prend $M \in \mathrm{GL}_3(\mathbb{F}_2)$, et on considère χ_M son polynôme caractéristique. Ce que l'on peut d'ores et déjà dire, c'est que χ_M est un polynôme unitaire de degré 3, et que X ne divise pas χ_M : M étant par hypothèse inversible, M ne peut avoir 0 pour valeur propre.
Commençons par écrire χ_M en produit de facteurs irréductibles : listons les polynômes de $\mathbb{F}_2[X]$ irréductibles unitaire de degré inférieur à 3 dont 0 n'est pas racine :
On trouve les quatre polynômes suivants :

$$X + 1 \qquad X^2 + X + 1 \qquad X^3 + X + 1 \qquad X^3 + X^2 + 1 \qquad (\heartsuit)$$

Listons ensuite les différents polynômes caractéristiques possibles. Pour ce faire, on combine les polynômes précédents pour obtenir des polynômes de degré 3 :

$$(X+1)^3 \qquad (X+1)\left(X^2 + X + 1\right) \qquad X^3 + X + 1 \qquad X^3 + X^2 + 1 \qquad (\clubsuit)$$

À partir de cette liste de polynômes caractéristiques possibles, on veut déterminer les polynômes minimaux des différents éléments de $\mathrm{GL}_3(\mathbb{F}_2)$. Pour ce faire, nous aurons besoin de quelques résultats préliminaires :

Proposition 1.1.2. *Soit E un k-espace vectoriel de dimension finie $n \geqslant 1$, et soit $f \in \mathscr{L}(E)$. Alors μ_f divise χ_f, et χ_f divise μ_f^n.*

Démonstration. Le fait que μ_f divise χ_f est une conséquence du théorème de Cayley-Hamilton.
On veut donc montrer l'autre point.
On travaille dans $k(X)$ le corps des fractions de $k[X]$, et on se sert de l'égalité suivante : dans $k(X)[Y]$, on a :

$$\forall m \in \mathbb{N}^*,\ X^m - Y^m = (X - Y)\left(X^{m-1} + X^{m-2}Y + \cdots + XY^{m-2} + Y^{m-1}\right)$$

Ainsi, si $\mu_f = \sum_{i=0}^{d} a_i X^i$, on a :

$$\begin{aligned}\mu_f(X) - \mu_f(Y) &= \sum_{i=0}^{d} a_i (X^i - Y^i) \\ &= \sum_{i=1}^{d} (X-Y)\left(a_i X^{i-1} + a_i X^{m-2} Y + \cdots + a_i Y^{d-1}\right) \\ &= (X-Y) \sum_{i=1}^{d} P_i Y^{i-1}\end{aligned}$$

avec $P_1, \cdots, P_d \in k[X]$. Après avoir fixé $\mathfrak{b}$ une base de E, on pose $M \overset{\text{def}}{=} \mathrm{Mat}(f, \mathfrak{b})$. On a $\mu_f(M) = 0$, et en utilisant le fait que $k \subseteq k(X)$, on regarde M comme un élément de $\mathcal{M}_n(k(X))$. On écrit dans $\mathcal{M}_n(k(X))$:

$$\mu_f(X)\,\mathrm{I}_n = (X\,\mathrm{I}_n - M)Q$$

avec $Q \overset{\text{def}}{=} P_1\,\mathrm{I}_n + P_1 M + \cdots + P_d M^{d-1} \in \mathcal{M}_n(k(X))$.
Prenons le déterminant de cette égalité, au sens $\det : \mathcal{M}_n(k(X)) \longrightarrow k(X)$. Il vient :

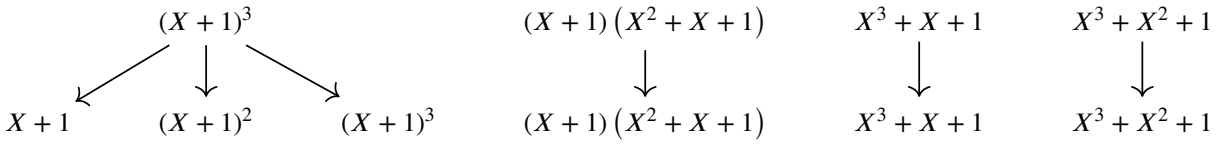
$$\mu_f^n = \chi_f \det(Q)$$

Or Q est par définition un élément de $\mathcal{M}_n(k[X])$, donc $\det(Q) \in k[X]$. Ainsi χ_f divise bien μ_f^n dans $k[X]$. □

Corollaire 1.1.3. *Sous les hypothèses de la proposition précédente, μ_f et χ_f partagent les mêmes diviseurs irréductibles.*

Démonstration. Soit $\pi \in k[X]$ un polynôme irréductible.
Si $\pi \mid \mu_f$ alors $\pi \mid \chi_f$ car $\mu_f \mid \chi_f$, et si $\pi \mid \chi_f$, alors $\pi \mid \mu_f^n$. Le lemme d'Euclide donne alors que $\pi \mid \mu_f$. □

Ce dernier résultat nous permet de dresser la liste des polynômes minimaux possibles pour les éléments de $\mathrm{GL}_3(\mathbb{F}_2)$. Reprenons la liste des polynômes caractéristiques donnée en (♣) : on cherche à chaque fois un polynôme minimal potentiel parmi les diviseurs des polynômes de (♣), en sachant qu'ils doivent posséder les mêmes facteurs irréductibles.
Ainsi, on a 6 polynômes minimaux possibles :



Pour chaque polynôme P parmi 6 les polynômes ci-dessus, on veut regarder à quoi ressemble un élément de $\mathrm{GL}_3(\mathbb{F}_2)$ qui aurait P pour polynôme minimal.

Afin de partir à l'assaut des trois premiers polynômes, nous allons utiliser la réduction de Jordan. On commence donc par une définition et le résultat principal de cette théorie de réduction des endomorphismes.

Définition 1.1.4 (Cellule de Jordan)**.** *On se place dans E un k-espace vectoriel de dimension finie $n \geqslant 1$. Soit $r \in \mathbb{N}^*$ et $\lambda \in k$. On appelle* cellule de Jordan de taille r associée à λ *la matrice de $\mathcal{M}_r(k)$:*

$$J_{r,\lambda} \overset{def}{=} \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

Théorème 1.1.5 (Réduction de Jordan). *On se place dans E un k-espace vectoriel de dimension $n \geqslant 1$. Soit $f \in \mathscr{L}(E)$ un endomorphisme de polynôme caractéristique χ_f scindé sur $k[X]$. Alors :*

1. *Il existe $r_1, \cdots, r_m \in \mathbb{N}^*$ tels que $r_1 + \cdots + r_m = n$, $\lambda_1, \cdots, \lambda_m \in \mathrm{Sp}_k(f)$ (éventuellement avec répétitions) des valeurs propres de f et une base $\mathfrak{b}$ de E telles que :*

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} J_{r_1,\lambda_1} & & \\ & \ddots & \\ & & J_{r_m,\lambda_m} \end{pmatrix}$$

   On dit que $\mathfrak{b}$ est une base de Jordan *pour f.*
   De plus, l'écriture est unique à l'ordre des cellules de Jordan près.[1]

2. *Le polynôme minimal μ_f est également scindé sur $k[X]$, et si on écrit*

$$\mu_f = \prod_{\lambda \in \mathrm{Sp}_k(f)} (X - \lambda)^{r_\lambda}$$

   alors la taille maximale d'une cellule de Jordan associée à la valeur propre λ est r_λ.

Dans notre cas, l'étude est grandement facilitée par le fait que la seule valeur propre possible pour un élément de $\mathrm{GL}_3(\mathbb{F}_2)$ est 1, puisque 0 ne peut être valeur propre. Ainsi en écrivant la forme de Jordan d'un endomorphisme de $\mathbb{F}_2^3$, nous n'utiliserons que des blocs J_{i1} avec $i \in [\![1, 3]\!]$.

Nous sommes prêts à étudier les trois premiers polynômes.

Soit $f \in \mathscr{L}\left(\mathbb{F}_2^3\right)$.

Si $\mu_f = X + 1$: alors $f + \mathrm{id} = 0$ donc $f = \mathrm{id}$, c'est-à-dire que pour toute base $\mathfrak{b}$ de $\mathbb{F}_2^3$ on a :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Si $\mu_f = (X + 1)^2$: alors la taille maximale d'une cellule de Jordan associé à la valeur propre 1 est 2 par le second point du *théorème 1.1.5*.
Or si tous les cellules de Jordan de f sont de taille 1, alors la matrice représentative de f dans une base quelconque est semblable à l'identité, donc $f = \mathrm{id}$, et $\mu_f = X + 1$, ce qui contredit l'unicité du polynôme minimal.
Ainsi f admet au moins une cellule de Jordan de taille 2. Pour écrire la forme de Jordan de f il nous ne nous manque plus qu'un bloc de taille 1, ainsi il existe une base $\mathfrak{b}$ de $\mathbb{F}_2^3$ telle que :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & \boxed{\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}} \end{pmatrix}$$

Si $\mu_f = (X + 1)^3$: alors pour les mêmes raisons que le cas précédent, la décomposition de Jordan de f ne peut-être constituée que de blocs de taille 1, et si un des blocs est de taille 2 alors nécessairement l'autre bloc est de taille 1, et dans ce cas on a $\mu_f = (X + 1)^2 \neq (X + 1)^3$... contradiction.
Ainsi f n'admet qu'une seule cellule de Jordan dans sa décomposition, et celui-ci est de taille 3, donc nécessairement on a qu'il existe une base $\mathfrak{b}$ de $\mathbb{F}_2^3$ telle que :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

On a donc traité le cas des trois premiers polynômes minimaux possibles.

Pour le suivant, nous faisons appel au lemme des noyaux, que nous rappelons ci-dessous.

Lemme 1.1.6 (Lemme des noyaux). *On se place dans E un k-espace vectoriel. Soient $P_1, \cdots, P_n$ des polynômes de $k[X]$ premiers entre eux deux à deux. Alors pour tout $f \in \mathscr{L}(E)$, on a :*

$$\ker\left(\left(\prod_{i=1}^{n} P_i\right)(f)\right) = \bigoplus_{i=1}^{n} \ker\left(P_i(f)\right)$$

Soit $f \in \mathscr{L}(\mathbb{F}_2^3)$ de polynôme minimal $\mu_f = (X+1)\left(X^2+X+1\right)$. Les deux facteurs de μ_f étant irréductibles, ils sont premiers entre eux deux à deux, et puisque $\mu_f(f) = 0$, on a $\ker\left(\mu_f(f)\right) = \mathbb{F}_2^3$. Le lemme des noyaux donne alors que :

$$\mathbb{F}_2^3 = \ker(f+1) \oplus \ker\left(f^2+f+1\right)$$

En particulier on a obtenu une décomposition en somme directe de $\mathbb{F}_2^3$ en deux sous espaces stables par f, à savoir $E_1 \overset{\text{def}}{=} \ker(f+1)$ et $E_2 \overset{\text{def}}{=} \ker\left(f^2+f+1\right)$.

On veut donc trouver une base convenable pour représenter f, en sachant qu'on pourra toujours le faire sous la forme :

$$\begin{pmatrix} \mathrm{Mat}\left(f_{|E_1}, \mathfrak{b}_1\right) & \\ & \mathrm{Mat}\left(f_{|E_2}, \mathfrak{b}_2\right) \end{pmatrix}$$

où $\mathfrak{b}_1$ et $\mathfrak{b}_2$ sont des bases respectives de E_1 et de E_2.

On a que $f_{|E_1} = \mathrm{id}_{E_1}$, donc quelque soit la base $\mathfrak{b}_1$ choisie, on a $\mathrm{Mat}\left(f_{|E_1}, \mathfrak{b}_1\right) = (1)$.

Pour déterminer une bonne base dans laquelle représenter $f_{|E_2}$, on introduit la notion de matrice compagnon.

Définition 1.1.7 (Matrice compagnon). *On se donne k un corps, et $P \in k[X]$ un polynôme unitaire non nul, disons $P = a_0 + a_1 X + \cdots a_{n-1}X^{n-1} + X^n$ avec $n = \deg P$. On appelle* matrice compagnon de P *la matrice $C_P \in \mathcal{M}_n(k)$:*

$$C_P \overset{def}{=} \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}$$

On peut désormais énoncer et démontrer un théorème qui nous sera utile pour représenter f, et dont nous pourrons nous servir pour traiter le cas des derniers polynômes minimaux.

Théorème 1.1.8. *Soit $f \in \mathscr{L}(k^n)$ un endomorphisme de polynôme minimal μ_f. Si μ_f est irréductible, alors il existe une base $\mathfrak{b}$ telle que la matrice représentative de f dans la base $\mathfrak{b}$ est diagonale par blocs, dont les blocs sont les matrices compagnons C_{μ_f}.*

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} C_{\mu_f} & & & \\ & C_{\mu_f} & & \\ & & \ddots & \\ & & & C_{\mu_f} \end{pmatrix}$$

Démonstration. Posons $E = k^n$. On suppose que le polynôme minimal μ_f est irréductible. On note d son degré, et on écrit $\mu_f = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d$. On considère $L \overset{\text{def}}{=} \dfrac{k[X]}{\left(\mu_f\right)}$.

Puisque k est un corps, $k[X]$ est principal et donc vérifie de lemme d'Euclide. Or μ_f est irréductible dans $k[X]$, donc premier dans $k[X]$ par lemme d'Euclide. Ainsi $\left(\mu_f\right)$ est un idéal premier de l'anneau principal $k[X]$, donc $\left(\mu_f\right)$ est maximal. Ainsi L est un corps. De plus, l'application suivante est bien définie :

$$\begin{array}{ccc} L \times E & \longrightarrow & E \\ (\overline{P}, v) & \longmapsto & \overline{P} \cdot v \overset{\text{def}}{=} \overline{P}(u)(v) \end{array}$$

Cette application munit E d'une structure de L-espace vectoriel. Posons $m \overset{\text{def}}{=} \dim_L(E)$, et prenons $(\mathfrak{e}_1, \cdots, \mathfrak{e}_m)$ une L-base de E.
Posons :

$$\mathfrak{b} = (\mathfrak{e}_1, f(\mathfrak{e}_1), \cdots, f^{d-1}(\mathfrak{e}_1), \mathfrak{e}_2, f(\mathfrak{e}_2), \cdots, f^{d-1}(\mathfrak{e}_2), \cdots, \mathfrak{e}_m, f(\mathfrak{e}_m), \cdots, f^{d-1}(\mathfrak{e}_m)) = \left(\rho_{ij}\right)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant d}}$$

Montrons que $\mathfrak{b}$ est une k-base de E.
Étant donné un vecteur $v \in E$, il existe une unique écriture de v sous la forme :

$$v = \sum_{i=1}^{m} \overline{P_i} \cdot \mathfrak{e}_i \qquad \left(\overline{P_i}\right)_{i \in [\![1,m]\!]} \in L^m$$

L'unicité de la division euclidienne par μ_f dans $k[X]$ nous donne que pour tout $i \in [\![1, m]\!]$, il existe un unique d-uplet $\left(c_{ij}\right)_{j \in [\![1,d]\!]} \in k^d$ tel que $\overline{P_i} = c_{i1} + c_{i2}\overline{X} + \cdots + c_{id}\overline{X}^{d-1}$. Alors :

$$v = \sum_{i=1}^{m} \overline{P_i} \cdot \mathfrak{e}_i = \sum_{i=1}^{m} \sum_{j=1}^{d} c_{ij} f^{j-1}(\mathfrak{e}_i) = \sum_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant d}} a_{ij}\rho_{ij}$$

Ainsi il existe une unique combinaison linéaire d'éléments de $\mathfrak{b}$ permettant s'écrire v, $\mathfrak{b}$ est donc une famille libre et génératrice : c'est une k-base de E.
On veut écrire la matrice de f dans la base $\mathfrak{b}$. Soit $i \in [\![1, m]\!]$, et soit $j \in [\![1, d]\!]$. On distingue deux cas :

Si $j \leqslant d-1$: alors le vecteur $\rho_{ij} = f^{j-1}(\mathfrak{e}_i)$ est envoyé sur $f(\rho_{ij}) = f^j(\mathfrak{e}_i) = \rho_{i,j+1}$.

Si $j = d$: alors $\rho_{ij} = f^{d-1}(\mathfrak{e}_i)$ est envoyé sur $f(\rho_{id}) = f^d(\mathfrak{e}_i)$. On se souvient alors que μ_f est le polynôme minimal de f, donc $\mu_f(f) = a_0 + a_1 f + \cdots + a_{d-1}f^{d-1} + f^d = 0$. En particulier, on a :

$$\mu_f(f)(\mathfrak{e}_i) = 0 = a_0\mathfrak{e}_i + a_1 f(\mathfrak{e}_i) + \cdots + a_{d-1}f^{d-1}(\mathfrak{e}_i) + f^d(\mathfrak{e}_i)$$
$$0 = a_0\rho_{i1} + a_1\rho_{i2} + \cdots + a_{d-1}\rho_{id} + f(\rho_{id})$$

Ainsi ρ_{id} est envoyé sur $-a_0\rho_{i1} - a_1\rho_{i2} - \cdots - a_{d-1}\rho_{id}$.

Ainsi, on a :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} \boxed{\begin{matrix} 0 & & & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & \ddots & 0 & -a_{d-2} \\ & & 1 & -a_{d-1} \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} 0 & & & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & \ddots & 0 & -a_{d-2} \\ & & 1 & -a_{d-1} \end{matrix}} \end{pmatrix}$$

□

Revenons-en à notre endomorphisme f. On regarde ici $f_{|E_2}$, dont le polynôme minimal est $X^2 + X + 1$, qui est irréductible sur $\mathbb{F}_2$. On peut trouver $\mathfrak{b}_2$ une base de E_2 dans laquelle l'endomorphisme $f_{|E_2}$ est représenté par la matrice :

$$\mathrm{Mat}\left(f_{|E_2}, \mathfrak{b}_2\right) = C_{X^2+X+1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Ainsi, il existe une base $\mathfrak{b}$ de $\mathbb{F}_2^3$, obtenue en concaténant les bases $\mathfrak{b}_1, \mathfrak{b}_2$, dans laquelle on peut représenter f par :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Il reste ainsi le cas des deux derniers polynômes minimaux possibles à traiter.

Soit $f \in \mathscr{L}\left(\mathbb{F}_2^3\right)$.

Si $\mu_f = X^3 + X + 1$: on utilise encore une fois le *théorème 1.1.8*. Ici, μ_f est irréductible sur $\mathbb{F}_2$, donc il existe une base $\mathfrak{b}$ telle que f soit représenté par la matrice compagnon de $X^3 + X + 1$, c'est-à-dire que l'on a :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Si $\mu_f = X^3 + X^2 + 1$: on procède de la même manière. Le *théorème 1.1.8* donne l'existence d'une base $\mathfrak{b}$ pour laquelle on a :

$$\mathrm{Mat}(f, \mathfrak{b}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Pour récapituler, les matrices suivantes sont des représentantes de toutes les classes de similitude de $\mathrm{GL}_3(\mathbb{F}_2)$.

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad M_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad M_4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad M_5 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad M_6 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Le groupe $\mathrm{GL}_3(\mathbb{F}_3)$ possède donc 6 classes de conjugaison, et on se propose de déterminer l'ordre des éléments de chaque classe.

Notation. *Pour $i \in [\![1, 6]\!]$, on notera C_{M_i} la classe de conjugaison de M_i.*

Remarque. *Si on prend $A \in \mathrm{GL}_3(\mathbb{F}_2)$ et si on trouve $n \in \mathbb{N}^*$ tel que $A^n = \mathrm{I}_3$, alors :*

$$\mathrm{o}(A) \in \left\{ k \in \mathbb{N}^* \;\middle|\; k \mid n \text{ et } k \geqslant \deg\left(\mu_A\right) \right\}$$

En effet, on sait par la théorie des groupes que $\mathrm{o}(A) \mid n$, mais $\mathrm{o}(A)$ ne peut-être plus petit que le degré du polynôme minimal de A, sinon on aurait que $X^{\mathrm{o}(A)} + 1$ est un polynôme annulateur de A de degré strictement plus petit que $\deg\left(\mu_A\right)$, contredisant ainsi l'hypothèse de minimalité de μ_A.

On peut ainsi calculer les ordres des éléments de chaque classe :

- C_{M_1} : On a que $M_1 = \mathrm{I}_3$, ainsi $C_{M_1} = \left\{\mathrm{I}_3\right\}$, et tous les éléments de C_{M_1} sont donc d'ordre 1.
- C_{M_2} : Si $A \in C_{M_2}$, alors :
$$\mu_A = (X + 1)^2 = X^2 + 1$$
Ainsi $A^2 = \mathrm{I}_3$, donc A est d'ordre 2.
- C_{M_3} : Soit $A \in C_{M_3}$. On a :
$$\mu_A = (X + 1)\left(X^2 + X + 1\right) = X^3 + 1$$
Donc $A^3 = \mathrm{I}_3$, c'est-à-dire que A est d'ordre 3.
- C_{M_4} : Si $A \in C_{M_4}$, alors :
$$\mu_A = (X + 1)^3 = X^3 + X^2 + X + 1$$
On a donc $A^3 + A^2 + A + \mathrm{I}_3 = 0$. En multipliant par A, on obtient $A^4 + A^3 + A^2 + A = 0$, mais $A^3 + A^2 + A = \mathrm{I}_3$, d'où $A^4 = \mathrm{I}_3$. Ainsi A est d'ordre 4.
- C_{M_5} : Soit $A \in C_{M_5}$. De nouveau, on a :
$$\mu_A = X^3 + X + 1$$
On a donc la relation $A^3 + A + \mathrm{I}_3 = 0$, et en multipliant par A^4, il vient que $A^7 + A^5 + A^4 = 0$.
En écrivant A^5 comme $A^2 \cdot A^3 = A^2\left(A + \mathrm{I}_3\right) = A^3 + A^2$, et aussi $A^4 = A \cdot A^3 = A\left(A + \mathrm{I}_3\right) = A^2 + A$, il vient $A^7 + A^3 + A^2 + A^2 + A = A^7 + A^3 + A = 0$, mais $A^3 + A = \mathrm{I}_3$, d'où $A^7 = \mathrm{I}_3$. Ainsi A est d'ordre 7.

- C_{M_6} : On prend $A \in C_{M_6}$, on a donc :
$$\mu_A = X^3 + X^2 + 1$$
Une fois encore, $A^3 + A^2 + \mathrm{I}_3 = 0$. Multiplions cette relation par A^{-3}. Il vient que $\mathrm{I}_3 + A^{-1} + A^{-3} = 0$, donc que A^{-1} est annulé par le polynôme $X^3 + X + 1$ qui est irréductible et unitaire donc minimal, ainsi $A^{-1} \in C_{M_5}$, et par le point précédent $\mathrm{o}\left(A^{-1}\right) = 7$. Ainsi A est également d'ordre 7.

Propriété. *Le groupe $\mathrm{GL}_3(\mathbb{F}_2)$ contient donc une classe d'un élément d'ordre 1, une classe d'éléments d'ordre 2, une classe d'éléments d'ordre 3, une classe d'éléments d'ordre 4 et deux classes d'éléments d'ordre 7 telles que les inverses des éléments de l'une des deux classes sont dans l'autre.*

1.1.2 Ordre des classes de conjugaison

Faisons agir $G \overset{\text{def}}{=} \mathrm{GL}_3(\mathbb{F}_2)$ sur lui-même par conjugaison. Si $x \in G$, alors on notera $\mathcal{O}_x$ l'orbite de x sous l'action de G. Notre but est de faire apparaître les classes de conjugaison de G, ce que nous faisons bien, puisque dans notre cas, on a :
$$\mathcal{O}_x = \{g \cdot x \mid g \in G\} = \left\{gxg^{-1} \;\middle|\; g \in \mathrm{GL}_3(\mathbb{F}_2)\right\} = C_x$$

On sait de plus, en notant $\mathrm{Stab}_G(x)$ le stabilisateur de x dans G, c'est-à-dire l'ensemble des éléments $g \in G$ tels que $g \cdot x = x$, que l'on a la relation suivante :
$$\forall x \in G, \quad |G| = \left|\mathrm{Stab}_G(x)\right| \cdot |\mathcal{O}_x|$$

C'est donc en connaissant le stabilisateur d'éléments bien choisis que nous parviendrons à déterminer le cardinal de chaque classe de conjugaison de $\mathrm{GL}_3(\mathbb{F}_2)$.

Or, on a une description plus pratique du stabilisateur d'un élément dans le cas de l'action par conjugaison :
$$\forall x \in \mathrm{GL}_3(\mathbb{F}_2), \quad \mathrm{Stab}_G(x) = \left\{g \in \mathrm{GL}_3(\mathbb{F}_2) \mid gxg^{-1} = x\right\} = \left\{g \in \mathrm{GL}_3(\mathbb{F}_2) \mid gx = xg\right\}$$

Le stabilisateur de x est ainsi l'ensemble des éléments qui commutent avec x, ce qui motive la définition suivante :

Définition 1.1.9 (Centralisateur)**.** *Si G est un groupe et que $X \subseteq G$, on appelle* centralisateur de X *l'ensemble des éléments qui commutent avec tout élément de X. On le notera $C_G(X)$.*
En particulier, lorsque X est réduit à un seul élément $x \in G$, on notera $C_G(x)$ au lieu de $C_G(\{x\})$: c'est l'ensemble des éléments de G qui commutent avec x.

Dans notre cas, on aura alors :
$$\forall i \in [\![1, 6]\!], \quad |C_{M_i}| = \frac{168}{\left|C_{\mathrm{GL}_3(\mathbb{F}_2)}(M_i)\right|}$$

On calcule ainsi le cardinal de l'ensemble des matrices de $\mathrm{GL}_3(\mathbb{F}_2)$ qui commutent avec un représentant de chaque classe de conjugaison.

Pour se faire, on peut pour chaque $i \in [\![1, 6]\!]$ commencer par prendre A dans $C_{\mathrm{GL}_3(\mathbb{F}_2)}(M_i)$, que l'on note en toute généralité :
$$A = \begin{pmatrix} a & b & c \\ d & x & f \\ g & h & y \end{pmatrix}$$

On commence ainsi à éliminer des possibilités en demandant aux coefficients de A d'être tels que $AM_i = M_iA$. On peut pour cela se servir d'un logiciel de calcul formel comme Xcas.

On renseigne M_i avec une simple ligne de code et l'instruction `solve` :

```
M=[[0,0,1],[1,0,1],[0,1,0]]
```

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

```
solve([[[a,b,c],[d,x,f],[g,h,y]]*M=M*[[a,b,c],[d,x,f],[g,h,y]]],[a,b,c,d,x,f,g,h,y])
```

```
[-g+y,g,h,h,y,g+h,g,h,y]
```

Exemple d'exécution avec $M = M_5$

Remarque. *Je note les coefficients de A avec les lettres $a, \cdots, d, \boldsymbol{x}, f, c \ldots, h, \boldsymbol{y}$ (et non avec e et i) pour éviter que le logiciel* Xcas *ne confonde les variables* `e` *et* `i` *avec la constante d'Euler e et avec le ı complexe.*

- C_{M_1} : Puisque $M_1 = I_3$, tous les éléments de $GL_3(\mathbb{F}_2)$ commutent avec I_3, et $C_{GL_3(\mathbb{F}_2)}(I_3) = GL_3(\mathbb{F}_2)$ qui est d'ordre 168. On retrouve ainsi que C_{M_1} est d'ordre $\frac{168}{168} = 1$ [1].
- C_{M_2} : Soit $A \in C_{GL_3(\mathbb{F}_2)}(M_2)$. L'exécution du script précédent par Xcas nous donne que A est de la forme :

$$A = \begin{pmatrix} a & 0 & c \\ d & y & f \\ 0 & 0 & y \end{pmatrix}$$

Cette matrice est de déterminant $\det A = ay^2$ (qui est égal à ay puisque nous sommes en caractéristique 2) donc $ay = 1$ par hypothèse sur A. Ainsi $a = y = 1$, et A s'écrit :

$$A = \begin{pmatrix} 1 & 0 & c \\ d & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

Les paramètres c, d et f sont libres, il reste ainsi $2^3 = 8$ choix possibles pour le triplet (c, d, f). Ainsi $\left|C_{GL_3(\mathbb{F}_2)}(M_2)\right| = 8$.

Il y a donc $\frac{168}{8} = 21$ éléments d'ordre 2 dans $GL_3(\mathbb{F}_2)$.

- C_{M_3} : Pour $A \in C_{GL_3(\mathbb{F}_2)}(M_3)$, Xcas nous donne que A est de la forme (en caractéristique 2) :

$$A = \begin{pmatrix} a & 0 & 0 \\ 0 & h+y & h \\ 0 & h & y \end{pmatrix}$$

Cette matrice est de déterminant $a(hy + h + y)$ qui doit valoir 1, donc $a = 1$ et $hy + h + y = 1$. Autrement dit, on a que $hy + h + y + 1 = (h + 1)(y + 1) = 0$, ce qui ne laisse que 3 choix possibles pour le couple (h, y), ainsi $\left|C_{GL_3(\mathbb{F}_2)}(M_3)\right| = 3$.

Il y a donc $\frac{168}{3} = 56$ éléments d'ordre 3 dans $GL_3(\mathbb{F}_2)$.

- C_{M_4} : De la même manière, on a que toute matrice $A \in C_{GL_3(\mathbb{F}_2)}(M_4)$ est de la forme :

$$A = \begin{pmatrix} y & f & c \\ 0 & y & f \\ 0 & 0 & y \end{pmatrix}$$

On a $\det A = y^3 = 1$ donc $y = 1$, et les paramètres f et c restent libres, il y a ainsi $2^2 = 4$ possibilités pour le couple (c, f), d'où $\left|C_{GL_3(\mathbb{F}_2)}(M_4)\right| = 4$.

Il y a donc $\frac{168}{4} = 42$ éléments d'ordre 4 dans $GL_3(\mathbb{F}_2)$.

1. On pouvait s'en douter... nous voilà rassurés !

- C_{M_5} : On aura $A \in C_{\mathrm{GL}_3(\mathbb{F}_2)}(M_5)$ de la forme (en caractéristique 2) :

$$A = \begin{pmatrix} g+y & g & h \\ h & y & g+h \\ g & h & y \end{pmatrix}$$

Cette matrice est de déterminant $\det A = ghy + gh + gy + hy + h + g + y$ qui doit valoir 1 par hypothèse sur A. Ainsi on a $ghy + gh + gy + hy + h + g + y + 1 = 0$ qui se factorise en $(g+1)(h+1)(y+1) = 0$, ce qui laisse 7 choix possibles pour le triplet (g, h, y).
Ainsi $\left|C_{\mathrm{GL}_3(\mathbb{F}_2)}(M_5)\right| = 7$.

Il y a donc $\dfrac{168}{7} = 24$ éléments dans C_{M_5}.

- C_{M_5} : On pourrait raisonner de la même manière, mais on pourrait aussi se souvenir que C_{M_6} contient les inverses des éléments de C_{M_5} et réciproquement (*voir propriété de la page 9*).
Ainsi l'application de passage à l'inverse réalise une bijection $C_{M_5} \simeq C_{M_6}$, ces deux classes ont donc le même cardinal : $\left|C_{\mathrm{GL}_3(\mathbb{F}_2)}(M_6)\right| = 7$.
Cela nous donne de plus qu'il y a $|C_{M_5} \sqcup C_{M_6}| = 24 + 24 = 48$ éléments d'ordre 7 dans $\mathrm{GL}_3(\mathbb{F}_2)$.

Remarque. *On a ainsi trouvé* 1 *élément d'ordre* 1, 21 *éléments d'ordre* 2, 56 *éléments d'ordre* 3, 42 *éléments d'ordre* 4 *et* 48 *éléments d'ordre* 7, *c'est-à-dire* $1 + 21 + 56 + 42 + 48 = 168$ *éléments au total... ouf!*

1.1.3 Simplicité de $\mathrm{GL}_3(\mathbb{F}_2)$

Nous sommes prêts à montrer la simplicité de $\mathrm{GL}_3(\mathbb{F}_2)$.

Prenons N un sous-groupe distingué de $\mathrm{GL}_3(\mathbb{F}_2)$, et supposons $N \neq \{\mathrm{I}_3\}$. Nous avons alors que N vérifie quelques propriétés :

Propriétés.

- *Pour tout $g \in N$, N contient toute la classe de conjugaison de g.*

  En effet, N est distingué donc il est stable par tout automorphisme intérieur.
- *Si N contient un élément d'ordre* 4, *alors il contient tous les éléments d'ordre* 2 *et d'ordre* 4.

  Cela vient du fait que si $g \in N$ est d'ordre 4, alors $g^2 \in N$ et g^2 est d'ordre 2. Par le point précédent, N contient alors à la fois toute la classe de g et la classe de g^2, et puisqu'il n'y a qu'une seule classe de conjugaison qui contient des éléments d'ordre 2 (respectivement 4), N contient tous les éléments d'ordre 2 (respectivement d'ordre 4).
- *Si N contient un élément d'ordre* 7, *alors il les contient tous.*

  En effet, si $g \in N$ est d'ordre 7 alors g^{-1} est aussi dans N et 7 contient alors la classe de g et la classe de g^{-1} qui sont distinctes par la *propriété de la page 9*. Ainsi N contient les classes C_{M_5} et C_{M_6} qui, à elles deux, contiennent tous les éléments d'ordre 7.

Posons $\alpha, \beta, \gamma, \delta \in \{0, 1\}$ des entiers qui représentent des variables booléennes de la façon suivante :

$\alpha = 1$ si et seulement si N contient des éléments d'ordre 2.
$\beta = 1$ si et seulement si N contient des éléments d'ordre 3.
$\gamma = 1$ si et seulement si N contient des éléments d'ordre 4.
$\delta = 1$ si et seulement si N contient des éléments d'ordre 7.

On peut alors reformuler la propriété précédente, et dire que N contient 1 élément d'ordre 1, 21α éléments d'ordre 2, 56β éléments d'ordre 3, 42γ éléments d'ordre 4 et 48δ éléments d'ordre 7 ; avec de plus :

$$\gamma = 1 \Longrightarrow \alpha = 1 \qquad (\heartsuit)$$

Le sous-groupe N est alors d'ordre $1 + 21\alpha + 56\beta + 42\gamma + 48\delta$. Sachant que cet ordre divise $|\mathrm{GL}_3(\mathbb{F}_2)| = 168$ par le théorème de Lagrange, on élimine petit à petit les possibilités.

Si $\alpha = 0$: par contraposée de (♥), on a que $\gamma = 0$, et donc N est d'ordre $1 + 56\beta + 48\delta$. Ayant supposé que N était non-trivial, il ne reste que 3 possibilités pour l'ordre de N :

$$|N| \in \{49, 57, 105\}$$

Or aucun de ces nombres ne divise 168, il est donc impossible que α soit nul :

Propriété. *On a $\alpha = 1$, N contient donc tous les éléments d'ordre 2.*

Si $\beta = 0$: on a alors que N est d'ordre $22 + 42\gamma + 48\delta$, donc on a :

$$|N| \in \{22, 64, 70, 112\}$$

Une fois encore, aucun de ses nombres ne divise 168, ainsi β ne peut valoir 0.

Propriété. *On a $\beta = 1$, N contient donc tous les éléments d'ordre 3.*

Si $\gamma = 0$: avec les informations des deux premiers points, on a que N est d'ordre $78 + 48\delta$, donc on a :

$$|N| \in \{78, 126\}$$

Pas un de ces nombres ne divise 168, ainsi γ vaut 1.

Propriété. *On a $\gamma = 1$, N contient donc tous les éléments d'ordre 4.*

Si $\delta = 0$: alors N ne peut être que d'ordre 120 qui ne divise pas 168, donc δ n'est pas nul.

Propriété. *On a $\delta = 1$, N contient donc tous les éléments d'ordre 7.*

On vient donc de montrer que N contient tous les éléments de tous ordres possibles, ainsi $N = \mathrm{GL}_3(\mathbb{F}_2)$. On en déduit le résultat principal de cette partie :

Théorème 1.1.10 (Existence d'un groupe simple d'ordre 168)**.** *Il existe un groupe simple d'ordre 168.*

Démonstration. Par ce qui précède, le groupe $\mathrm{GL}_3(\mathbb{F}_2)$ est un groupe simple d'ordre 168. □

1.2 Le groupe spécial projectif linéaire PSL(E)

Soit k un corps, et E un k-espace vectoriel de dimension finie $n \geqslant 1$.

On note $\mathrm{SL}(E)$ l'ensemble des éléments du groupe linéaire $\mathrm{GL}(E)$ dont le déterminant vaut 1 : c'est un groupe pour la composition que l'on appelle *groupe spécial linéaire*, et dans le cas où $E = k^n$, on le notera $\mathrm{SL}_n(k)$.

Le déterminant étant un invariant de conjugaison, on a de plus que $\mathrm{SL}(E) \lhd \mathrm{GL}(E)$.

1.2.1 Généralités sur le groupe spécial linéaire SL(E)

Définition 1.2.1 (Transvection)**.** *Sous l'hypothèse où E est un k-espace vectoriel de dimension $n \geqslant 2$, si H est un hyperplan de E et D une droite de E vérifiant $D \subseteq H$, on appelle* transvection de droite D et d'hyperplan H *tout endomorphisme $u \in \mathscr{L}(E) \setminus \{\mathrm{id}_E\}$ tel que :*

1. $u_{|H} = \mathrm{id}_H$
2. $\forall x \in D,\ u(x) - x \in D$

Avec l'identification $E \simeq k^n$, on peut montrer que les transvections sont des endomorphismes que l'on peut représenter, dans une bonne base, par une matrice de la forme

$$T_{ij}(\lambda) \overset{\text{def}}{=} \begin{pmatrix} 1 & & & & \\ & \ddots & & \boxed{\lambda} & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow i \\ \\ \\ \end{matrix}, \quad j \downarrow$$

avec $i \neq j$ et $\lambda \in k^\times$.

En particulier, les transvections sont des éléments de SL(E).[5]

Proposition 1.2.2 (Centre de SL(E))**.** *Si E est un k-espace vectoriel de dimension n, alors le centre de* GL(E) *est formé des homothéties de rapport $\lambda \in k^\times$. De plus, on a :*

$$\begin{aligned} Z(\mathrm{SL}(E)) &= Z(\mathrm{GL}(E)) \cap \mathrm{SL}(E) \\ &= \left\{ \lambda \,\mathrm{id}_E \;\middle|\; \lambda \in k^\times, \lambda^n = 1 \right\} \end{aligned}$$

En particulier, Z(SL(E)) est un groupe isomorphe à un sous-groupe des racines n-ième de l'unité $\mathbb{U}_n$.[1]

Proposition 1.2.3 (Générateurs de SL(E))**.** *Dans le cas où $n \geqslant 2$, le groupe* SL(E) *est engendré par les transvections.*[1]

Proposition 1.2.4 (Conjugaison de transvections)**.** *Soit* $\mathbf{e}$ *une base de E. Pour tout $\lambda \in k^\times$, on note $t_\lambda \in$ SL(E) la transvection dont la matrice représentative dans la base* $\mathbf{e}$ *est $T_{1,2}(\lambda)$. Alors :*

1. *Toute transvection est conjuguée à t_1 dans* GL(E)*, et en particulier, toutes les transvections sont conjuguées dans* GL(E).
2. *Toute transvection est conjuguée à t_λ dans* SL(E) *pour une certaine valeur de $\lambda \in k^\times$.*[1]

Définition 1.2.5 (Commutateurs et groupe dérivé)**.** *Soit G un groupe et $x, y \in G$. On appelle* commutateur de x et y *l'élément :*

$$[x, y] \overset{def}{=} xyx^{-1}y^{-1}$$

On appelle groupe dérivé de G *le groupe engendré par les commutateurs. On le notera* $[G, G]$.

Remarques.

- *On a toujours $[G, G] \lhd G$. En effet, si $[x, y] \in [G, G]$ et $g \in G$, alors :*

$$\begin{aligned} g[x, y]g^{-1} &= gx\left(g^{-1}g\right)y\left(g^{-1}g\right)x^{-1}\left(g^{-1}g\right)y^{-1}g^{-1} \\ &= \left(gxg^{-1}\right)\left(gyg^{-1}\right)\left(gxg^{-1}\right)^{-1}\left(gyg^{-1}\right)^{-1} \\ &= \left[gxg^{-1}, gyg^{-1}\right] \in [G, G] \end{aligned}$$

- *Le groupe dérivé est trivial si et seulement si G est abélien, et le groupe quotient $G/[G, G]$ est abélien par construction. Le groupe dérivé est même le plus petit sous-groupe distingué de G tel que le quotient de G par le sous-groupe soit abélien.*

Proposition 1.2.6. *Supposons que $n \geqslant 2$, et $|k| \geqslant 4$ dans le cas où $n = 2$. Alors* [SL(E), SL(E)] = SL(E).

Démonstration. Le groupe SL(E) étant engendré par les transvections *(voir proposition 1.2.3)*, on veut montrer que toute transvection est dans [SL(E), SL(E)].
Puisque [SL(E), SL(E)] est distingué dans SL(E) qui est lui même distingué dans GL(E), et puisque les transvections sont conjuguées dans GL(E) (*voir proposition 1.2.4*), nous avons que si [SL(E), SL(E)] contient une transvection, alors il les contient toutes.
Montrons que [SL(E), SL(E)] contient une transvection.

- Si $|k| \geqslant 4$, on peut prendre $\lambda \in k \setminus \{0, \pm 1\}$, et après avoir fixé une base $\mathbf{e}$ de E, on pose u et v les endomorphismes

de SL(E) dont les matrices représentatives respectives dans la base $\mathfrak{e}$ sont :

$$U = \begin{pmatrix} \mathrm{I}_{n-2} & & \\ & \lambda & \\ & & \lambda^{-1} \end{pmatrix} \qquad \text{et} \qquad V = \begin{pmatrix} \mathrm{I}_{n-2} & & \\ & 1 & 1 \\ & 0 & 1 \end{pmatrix}$$

On pose $w \overset{\text{def}}{=} [u, v] \in [\mathrm{SL}(E), \mathrm{SL}(E)]$ dont la matrice représentative dans la base $\mathfrak{e}$ est

$$W = UVU^{-1}V^{-1} = \begin{pmatrix} \mathrm{I}_{n-2} & & \\ & 1 & \lambda^2 - 1 \\ & 0 & 1 \end{pmatrix}$$

Or $\lambda^2 - 1 \neq 0$, donc w est une transvection.

- Si $|k| \in \{2, 3\}$ et $n \geqslant 3$. On pose $u, v \in \mathrm{SL}(E)$ les endomorphismes dont les matrices respectives dans une base $\mathfrak{e} = (e_i)_{1 \leqslant i \leqslant n}$ sont :

$$U = \begin{pmatrix} \mathrm{I}_{n-3} & & & \\ & 1 & 0 & 1 \\ & 0 & 1 & 0 \\ & 0 & 0 & 1 \end{pmatrix} \qquad \text{et} \qquad V = \begin{pmatrix} \mathrm{I}_{n-3} & & & \\ & 0 & -1 & 0 \\ & 1 & 0 & 0 \\ & 0 & 0 & 1 \end{pmatrix}$$

De même, on pose $w \overset{\text{def}}{=} [u, v] \in [\mathrm{SL}(E), \mathrm{SL}(E)]$ dont la matrice représentative dans la base $\mathfrak{e}$ est :

$$W = UVU^{-1}V^{-1} = \begin{pmatrix} \mathrm{I}_{n-3} & & & \\ & 1 & 0 & 1 \\ & 0 & 1 & -1 \\ & 0 & 0 & 1 \end{pmatrix}$$

On pose ensuite $H \overset{\text{def}}{=} \ker(w - \mathrm{id}_E)$. C'est un hyperplan engendré par $e_1, \cdots, e_{n-1}$; et on pose également $D \overset{\text{def}}{=} \mathrm{Vect}_k(e_{n-2} - e_{n-1})$. On a $D \subseteq H$ et w est une transvection de droite D et d'hyperplan H.

Ainsi $[\mathrm{SL}(E), \mathrm{SL}(E)]$ contient une transvection, donc $[\mathrm{SL}(E), \mathrm{SL}(E)] = \mathrm{SL}(E)$. □

Proposition 1.2.7. *Soit $u \in \mathscr{L}(E)$ un endomorphisme stabilisant toute droite de E. Alors u est une homothétie, et $u \in Z(\mathrm{GL}(E))$.*[1]

1.2.2 Simplicité du groupe spécial projectif linéaire PSL(E)

Définition 1.2.8 (Groupe spécial projectif linéaire)**.** *On appelle* groupe spécial projectif linéaire *le quotient du groupe spécial linéaire par son centre, et on le note* PSL(E) *:*

$$\mathrm{PSL}(E) \overset{def}{=} \mathrm{SL}(E)/Z(\mathrm{SL}(E))$$

Théorème 1.2.9 (Simplicité de PSL(E))**.** *Si $n \geqslant 2$ et que $|k| \geqslant 4$ dans le cas où $n = 2$, alors le groupe* PSL(E) *est simple.*

Démonstration. Le groupe PSL(E) étant construit comme le quotient de SL(E) par son centre, les sous-groupes distingués de PSL(E) sont en bijection avec les sous-groupes distingués de SL(E) qui contiennent $Z(\mathrm{SL}(E))$. Il nous faut donc montrer qu'il y a que deux ce ces sous-groupes, à savoir $Z(\mathrm{SL}(E))$ et SL(E).
On pose X l'ensemble des droites de E, et on fait agir SL(E) sur X par l'action :

$$\begin{array}{ccc} \mathrm{SL}(E) \times X & \longrightarrow & X \\ (u, D) & \longmapsto & u(D) \end{array}$$

Lemme intermédiaire (Double transitivité de l'action)**.** *Étant données quatre droites $D_1, D_2, \Delta_1, \Delta_2$ avec $D_1 \neq D_2$ et $\Delta_1 \neq \Delta_2$, il existe $u \in \mathrm{SL}(E)$ tel que :*

$$u(D_1) = \Delta_1 \quad \text{et} \quad u(D_2) = \Delta_2$$

Pour ce faire, on choisit e_1, e_2, f_1 et f_2 des vecteurs non nuls et qui engendrent respectivement les droites D_1, D_2, Δ_1 et Δ_2. Puisque $D_1 \neq D_2$ et $\Delta_1 \neq \Delta_2$, les familles (e_1, e_2) et (f_1, f_2) sont libres, et on les complète en deux bases $\mathfrak{e} = (e_1, \cdots, e_n)$ et $\mathfrak{f} = (f_1, \cdots, f_n)$ de E.
On considère alors $u_0 \in \mathrm{GL}(E)$ l'automorphisme qui envoie la base $\mathfrak{e}$ sur la base $\mathfrak{f}$.
On pose également $\lambda \overset{\text{def}}{=} \det(u_0)^{-1}$, et on pose $u \in \mathrm{GL}(E)$ l'endomorphisme défini par :

$$u(e_1) = \lambda f_1 \quad \text{et} \quad \forall i \in [\![2, n]\!],\ u(e_i) = f_i$$

On a $\det(u) = \lambda \det(u_0) = 1$, donc $u \in \mathrm{SL}(E)$, et, comme souhaité, on a bien $u(D_1) = \Delta_1$ et $u(D_2) = \Delta_2$.
En particulier, l'action de $\mathrm{SL}(E)$ sur X est transitive.

On choisit une fois pour toute D une droite de E, et on pose :

$$H \overset{\text{def}}{=} \mathrm{Stab}_{\mathrm{SL}(E)}(D) = \{u \in \mathrm{SL}(E) \mid u(D) = D\}$$

Soit $N \lhd \mathrm{SL}(E)$ contenant $Z(\mathrm{SL}(E))$. On veut montrer que $N = Z(\mathrm{SL}(E))$ ou que $N = \mathrm{SL}(E)$.

— Cas où $N \subseteq H$: soit $v \in N$ et $\Delta \in X$. Par transitivité de l'action de $\mathrm{SL}(E)$ sur X, il existe $u \in \mathrm{SL}(E)$ tel que $u(D) = \Delta$. Puisque $N \lhd \mathrm{SL}(E)$, $u^{-1} \circ v \circ u \in N \subseteq H$, donc $u^{-1} \circ v \circ u$ stabilise D, et il vient :

$$v(\Delta) = v(u(D)) = u\left(\left(u^{-1} \circ v \circ u\right)(D)\right) = u(D) = \Delta$$

Ainsi v stabilise n'importe quelle droite de E, c'est donc une homothétie et un élément de $Z(\mathrm{SL}(E))$ par la *proposition 1.2.7*, d'où $Z(\mathrm{SL}(E)) \subseteq N \subseteq Z(\mathrm{SL}(E))$, c'est-à-dire $N = Z(\mathrm{SL}(E))$.

— Cas où $N \nsubseteq H$: on procède en plusieurs étapes.

• **Étape 1.** Montrons que $\mathrm{SL}(E) = NH$.

Puisque $N \lhd \mathrm{SL}(E)$, il nous suffit de montrer que $\mathrm{SL}(E) = \langle N, H \rangle$. En effet, NH est un sous-groupe de $\mathrm{SL}(E)$ par le deuxième théorème d'isomorphisme, NH est donc un sous-groupe contenant N et H, d'où $\langle N, H \rangle \subseteq NH$, et finalement $\langle N, H \rangle = NH$, l'autre inclusion étant évidente.

Soit $v_0 \in N \setminus H$ et $D_1 \overset{\text{def}}{=} v_0(D)$. Puisque $v_0 \notin H$, on a $D_1 \neq D$.

On prend $u \in \mathrm{SL}(E)$ et on pose $D_2 \overset{\text{def}}{=} u(D)$.

— Si $D_2 = D$, on a $u \in H \subseteq \langle N, H \rangle$.

— Si $D_2 \neq D$, le lemme en début de preuve nous donne l'existence de $v \in \mathrm{GL}(E)$ tel que $v(D_1) = D_2$ et $v(D) = D$, autrement dit on a $v \in H$ tel que $v(D_1) = D_2$. il vient alors :

$$u(D) = D_2 = v(D_1) = v(v_0(D))$$

Vu autrement, on a que l'endomorphisme $w \overset{\text{def}}{=} \left(v \circ v_0\right)^{-1} \circ u$ stabilise D, c'est-à-dire que $w \in H$. Mais alors $u = v \circ v_0 \circ w \in H \subseteq \langle N, H \rangle$.

Ainsi, $\mathrm{SL}(E) \subseteq \langle N, H \rangle \subseteq \mathrm{SL}(E)$, d'où $\mathrm{SL}(E) = \langle N, H \rangle = NH$.

• **Étape 2.** On pose :

$$A \overset{\text{def}}{=} \left\{ u \in \mathrm{SL}(E) \;\middle|\; \mathrm{Im}(u - \mathrm{id}_E) \subseteq D,\ u_{|D} = \mathrm{id}_D \right\}$$

Montrons que $A \lhd H$ et que A est abélien.
Soit $\mathfrak{e} = (e_1, \cdots, e_n)$ une base de E telle que $D = \mathrm{Vect}_k(e_1)$. Alors on a d'une part :

$$H = \left\{ u \in \mathrm{SL}(E) \;\middle|\; \mathrm{Mat}(u, \mathfrak{e}) = \begin{pmatrix} \det(M)^{-1} & \clubsuit \\ 0 & M \end{pmatrix},\ M \in \mathrm{GL}_{n-1}(k) \right\}$$

D'autre part :

$$A = \left\{ u \in \mathrm{SL}(E) \;\middle|\; \mathrm{Mat}(u, \mathfrak{e}) = \begin{pmatrix} 1 & \heartsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix} \right\}$$

Il est alors clair que A est un sous-groupe de H. C'est une partie de H (il suffit de prendre $M = \mathrm{I}_{n-1}$ dans la description de H donnée ci-dessus) non vide car elle contient l'identité, et puisque l'inverse d'une matrice triangulaire supérieure est une matrice triangulaire supérieure dont les coefficients diagonaux ont été inversés, on a que A est stable par produit et par passage à l'inverse : A est un sous-groupe de H.

Montrons que $A \lhd H$.

Soit $u \in A$ et $v \in H$. Notons U, V leurs matrices respectives dans la base $\mathfrak{e}$. Il existe donc $M \in \mathrm{GL}_{n-1}(k)$ telle que $V = \begin{pmatrix} \det(M)^{-1} & \clubsuit \\ 0 & M \end{pmatrix}$, et V^{-1} est alors de la forme $\begin{pmatrix} \det(M) & \spadesuit \\ 0 & M^{-1} \end{pmatrix}$. Il vient alors :

$$VUV^{-1} = \begin{pmatrix} \det(M)^{-1} & \clubsuit \\ 0 & M \end{pmatrix} \begin{pmatrix} 1 & \heartsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix} \begin{pmatrix} \det(M) & \spadesuit \\ 0 & M^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \diamondsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix}$$

où $\clubsuit, \heartsuit, \spadesuit$ et $\diamondsuit$ sont des vecteurs lignes non précisés. Ainsi l'endomorphisme $v \circ u \circ v^{-1}$ admet une matrice représentative dans la base $\mathfrak{e}$ de la forme souhaitée : $v \circ u \circ v^{-1} \in A$, donc le sous-groupe A est bien distingué dans H.

Montrons que A est abélien.

Soient encore une fois $u, v \in A$, de matrices représentatives respectives U et V dans la base $\mathfrak{e}$. Il existe ainsi $\heartsuit$ et $\diamondsuit$ deux vecteurs lignes tels que :

$$U = \begin{pmatrix} 1 & \heartsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & \diamondsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix}$$

Alors :

$$UV = \begin{pmatrix} 1 & \heartsuit + \diamondsuit \\ 0 & \mathrm{I}_{n-1} \end{pmatrix} = VU$$

Le sous-groupe A est donc abélien et distingué dans H.

Montrons ensuite que $\mathrm{SL}(E) = NA$. Comme pour l'**Étape 1**, on montre que $\mathrm{SL}(E) = \langle N, A \rangle$. On a que A contient toutes les transvections t_λ dont la matrice représentative dans la base $\mathfrak{e}$ est $T_{1,2}(\lambda)$ avec $\lambda \in k^\times$, or toute transvection est conjuguée à de telles transvections t_λ *(voir proposition 1.2.4)*, ainsi $\mathrm{SL}(E)$ est engendré par les conjugués des éléments de A, d'où :

$$\mathrm{SL}(E) = \left\langle uau^{-1} \;\middle|\; a \in A, u \in \mathrm{SL}(E) \right\rangle$$

Or, par l'**Étape 1**, nous pouvons écrire un élément de $\mathrm{SL}(E)$ sous la forme d'un produit d'un élément de N par un élément de H, ce qui nous donne :

$$\begin{aligned} \mathrm{SL}(E) &= \left\langle (vh)a(vh)^{-1} \;\middle|\; a \in A, v \in N, h \in H \right\rangle \\ &= \left\langle v\left(hah^{-1}\right)v^{-1} \;\middle|\; a \in A, v \in N, h \in H \right\rangle \end{aligned}$$

Or $A \lhd H$, d'où $\mathrm{SL}(E) \subseteq \langle N, A \rangle$. L'autre inclusion est triviale, et on a bien $\mathrm{SL}(E) = \langle N, A \rangle = NA$.

• **Étape 3.** On veut appliquer le deuxième théorème d'isomorphisme en utilisant le résultat de l'**Étape 2** : N est distingué dans $NA = \mathrm{SL}(E)$, d'où :

$$\mathrm{SL}(E)/N \simeq A/(N \cap A)$$

Puisque A est abélien, $\mathrm{SL}(E)/N$ l'est également, donc pour tout $u, v \in \mathrm{SL}(E)$, on a :

$$\overline{[u,v]} = \overline{u}\,\overline{v}\,\overline{u}^{\,-1}\,\overline{v}^{\,-1} = \overline{\mathrm{id}_E}$$

Donc $[u, v] \in N$, quelque soient $u, v \in \mathrm{SL}(E)$, d'où $[\mathrm{SL}(E), \mathrm{SL}(E)] \subseteq N$. Mais puisque $n \geqslant 2$, et que $|k| \geqslant 4$ si $n = 2$ par hypothèse, la *proposition 1.2.6* nous donne que $[\mathrm{SL}(E), \mathrm{SL}(E)] = \mathrm{SL}(E)$, d'où $N \subseteq \mathrm{SL}(E)$, c'est-à-dire $N = \mathrm{SL}(E)$.

Finalement N est toujours soit $Z(\mathrm{SL}(E))$ soit $\mathrm{SL}(E)$: le groupe $\mathrm{PSL}(E)$ est donc simple. □

1.2.3 Le cas $\mathrm{PSL}_2(\mathbb{F}_7)$

On se propose de regarder plus en détail le groupe projectif linéaire $\mathrm{PSL}_2(\mathbb{F}_7)$. Donnons-en une description rapide : il s'agit, par définition, du groupe spécial linéaire $\mathrm{SL}_2(\mathbb{F}_7)$ quotienté par son centre. On commence donc par décrire $Z(\mathrm{SL}_2(\mathbb{F}_7))$.

La *proposition 1.2.2* nous rappelle que le centre de $\mathrm{SL}_2(\mathbb{F}_7)$ est l'ensemble des homothéties de rapport $\lambda \in \mathbb{F}_7^\times$ de déterminant 1, c'est-à-dire :

$$Z(\mathrm{SL}(E)) = \left\{ \lambda \,\mathrm{id}_{\mathbb{F}_7^2} \;\middle|\; \lambda \in \mathbb{F}_7^\times, \lambda^2 = 1 \right\} = \left\{ \pm \mathrm{id}_{\mathbb{F}_7^2} \right\}$$

On a donc :

$$\mathrm{PSL}_2(\mathbb{F}_7) = \mathrm{SL}_2(\mathbb{F}_7) \Big/ \left\{ \pm \mathrm{id}_{\mathbb{F}_7^2} \right\} \qquad (\bigstar)$$

Penchons-nous sur $\mathrm{SL}_2(\mathbb{F}_7)$:

Théorème 1.2.10 (Cardinal de $\mathrm{SL}_n(\mathbb{F}_p)$)**.** *Soit $n \in \mathbb{N}$ et $p \in \mathbb{F}_p$. Alors :*

$$|\mathrm{SL}_n(\mathbb{F}_p)| = \frac{1}{p-1} \prod_{k=1}^{n} \left(p^n - p^{k-1}\right)$$

Démonstration. Le déterminant $\det : \mathrm{GL}_n(\mathbb{F}_p) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{F}_p^\times$ est un morphisme surjectif, de noyau $\ker \det = \mathrm{SL}_n(\mathbb{F}_p)$, ainsi par le premier théorème d'isomorphisme nous avons :

$$\mathrm{GL}_n(\mathbb{F}_p) / \mathrm{SL}_n(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$$

En terme de cardinal, et sachant l'ordre de $\mathrm{GL}_n(\mathbb{F}_p)$ (*théorème* **??**), il vient :

$$|\mathrm{SL}_n(\mathbb{F}_p)| = \frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|\mathbb{F}_p^\times|} = \frac{1}{p-1} \prod_{k=1}^{n} \left(p^n - p^{k-1}\right)$$

□

En particulier, on a :

$$|\mathrm{SL}_2(\mathbb{F}_7)| = \frac{1}{7-1}\left(7^2-1\right)\left(7^2-7\right) = \frac{48 \cdot 42}{6} = 336$$

Il vient donc, en écrivant ($\bigstar$) en terme de cardinal :

$$|\mathrm{PSL}_2(\mathbb{F}_7)| = \frac{|\mathrm{SL}_2(\mathbb{F}_7)|}{2} = \frac{336}{2} = 168$$

Cela nous donne une autre preuve du théorème de cette section :

Théorème 1.2.11 (Existence d'un groupe simple d'ordre 168)**.** *Il existe un groupe simple d'ordre 168.*

Démonstration. Par ce qui précède, le groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ est d'ordre 168, et le *théorème 1.2.9* nous donne que ce groupe est simple. □

1.3 Un isomorphisme entre $\mathrm{GL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$?

1.3.1 Espace projectif

Définition 1.3.1 (Relation de colinéarité)**.** *Soient k un corps et E un k-espace vectoriel non trivial.*
Si $x, y \in E \setminus \{0\}$, on définit la relation $\sim$ par :

$$x \sim y \iff \exists \lambda \in k^*,\ y = \lambda x$$

Proposition 1.3.2. *La relation $\sim$ est une relation d'équivalence.*

Démonstration. Soient x et y sont des vecteurs non nuls de E.
La réflexivité de la relation $\sim$ est évidente puisque $x = 1 \cdot x$ et $1 \in k^\times$.
Pour la symétrie, il suffit de considérer $\mu = \lambda^{-1} \in k^\times$ pour avoir $x = \mu y$, où $\lambda \in k^\times$ est tel que $y = \lambda x$.
Enfin pour la transitivité, prenons z un troisième vecteur non nul et on suppose que $x \sim z$ et $y \sim z$, c'est-à-dire qu'il existe $\lambda, \lambda' \in k^\times$ tels que $z = \lambda x = \lambda' y$. Mais alors $y = \mu x$ avec $\mu = \lambda \cdot \lambda'^{-1} \in k^\times$, donc $x \sim y$.
La relation $\sim$ est donc bien une relation d'équivalence. □

Définition 1.3.3 (Espace projectif)**.** *On appelle* espace projectif *le quotient $E \setminus \{0\} / \sim$, et on le note $\mathbb{P}(E)$. C'est l'ensemble des droites vectorielles de E.*
Dans le cas où E est de dimension finie $\dim_k(E) = n+1 \geqslant 0$, on dira que $\mathbb{P}(E)$ est de dimension finie *égale à n.* [2]

Notation. *Si $E = k^{n+1}$, on notera aussi $\mathbb{P}^n(k)$ au lieu de $\mathbb{P}\left(k^{n+1}\right)$.*

On s'intéressera ici plus particulièrement au cas de la dimension 1, c'est-à-dire au cas de la *droite projective*. Pour $E = k^2$, la droite projective contient les droites $\mathrm{Vect}_k \begin{pmatrix} x \\ y \end{pmatrix}$. Pour $x, y \in k$, on distingue deux cas :

Si $x \neq 0$: alors la droite $\mathrm{Vect}_k \begin{pmatrix} x \\ y \end{pmatrix}$ est aussi engendrée par $\begin{pmatrix} 1 \\ z \end{pmatrix}$ avec $z = x^{-1}y$. En particulier, on peut représenter toute droite engendrée par un vecteur de première coordonnée non nulle par un élément de k. Mais il nous manque toujours une dernière droite :

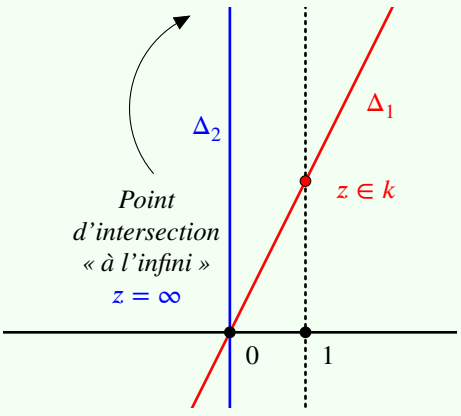
Si $x = 0$: alors la droite $\mathrm{Vect}_k \begin{pmatrix} 0 \\ y \end{pmatrix}$ est aussi engendrée par $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Nous la représenterons par le symbole « ∞ ».

On pose $\widehat{k} \overset{\text{def}}{=} k \cup \{\infty\}$. Par ce qui précède, on peut alors identifier $\widehat{k}$ et $\mathbb{P}^1(k)$ par l'application :

$$\begin{array}{ccc} \widehat{k} & \longrightarrow & \mathbb{P}^1(k) \\ z & \longmapsto & \begin{cases} \mathrm{Vect}_k \begin{pmatrix} 1 \\ z \end{pmatrix} & \text{si } z \neq \infty \\ \mathrm{Vect}_k \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \text{si } z = \infty \end{cases} \end{array}$$

Cette application est bijective par notre disjonction de cas précédente.

Remarque. *Comment se représenter $\mathbb{P}^1(k)$?*
On commence par se donner Δ_1 et Δ_2 deux droites vectorielles de k^2.



Afin de représenter chaque cas, on suppose que Δ_2 est une droite verticale, mais pas Δ_1, comme sur le dessin ci-contre. Pour construire $\widehat{k}$, on considère les points d'intersection d'une droite de $\mathbb{P}^1(k)$ avec la droite d'équation $x = 1$.

- *Pour la droite Δ_1, ce point est un élément z de k (point rouge ● sur le schéma), qui se trouve aussi être dans $\widehat{k} = k \cup \{\infty\}$.*
- *Pour Δ_2, il n'y a pas à proprement parler de point d'intersection : on considère donc que cette intersection se trouve « à l'infini », ce qui nous donne l'élément $\infty \in \widehat{k} = k \cup \{\infty\}$.*

Ce procédé est en quelque sorte la projection stéréographique d'une droite de $\mathbb{P}^1(k)$ sur la droite $x = 1$.

On veut désormais regarder les automorphismes de $\mathbb{P}^1(k)$.

2. L'espace projectif se déduit d'un espace vectoriel, le mot « dimension » ne fait donc référence qu'à la dimension de cet espace vectoriel.

Notation. *Si $v \in k^2 \setminus \{0\}$ est un vecteur non nul, on notera $[v]$ la droite qu'il représente dans $\mathbb{P}^1(k)$, autrement dit, on pose :*

$$\begin{bmatrix} x \\ y \end{bmatrix} \overset{def}{=} \left\{ \lambda \begin{pmatrix} x \\ y \end{pmatrix} \;\middle|\; \lambda \in k \right\}$$

Définition 1.3.4 (Groupe projectif)**.** *On appelle* groupe projectif de $\mathbb{P}^1(k)$ *le groupe* $\mathrm{GL}_2(k)/\{\lambda\,\mathrm{id} \mid \lambda \in k^\times\}$. *On le note* $\mathrm{PGL}_2(k)$.

Notation. *Si $M \in \mathrm{GL}_2(k)$, on notera $[M]$ sa classe dans $\mathrm{PGL}_2(k)$, c'est-à-dire que l'on a :*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \overset{def}{=} \left\{ \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \lambda \in k^\times \right\}$$

Proposition 1.3.5. *Le groupe projectif $\mathrm{PGL}_2(k)$ agit sur $\mathbb{P}^1(k)$ par :*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$$

Définition 1.3.6 (Homographie)**.** *On appelle* homographie *toute bijection de $\mathbb{P}^1(k)$ obtenue en faisant agir un élément de $\mathrm{PGL}_2(k)$ par l'action précédente.*

Plus explicitement, les homographies sont des fonctions de la forme :

$$f : \begin{cases} \widehat{k} & \longrightarrow & \widehat{k} \\ x & \longmapsto & \dfrac{ax+b}{cx+d} \end{cases} \quad \text{où} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(k) \tag{1}$$

Ici, la division par $cx + d$ signifie la multiplication par $(cx + d)^{-1}$ dans k, avec les règles de calcul suivantes :

— La division par 0 d'un élément non nul donne ∞.

— La division par ∞ d'un élément différent de ∞ donne 0.

On a en particulier que $f(\infty) = \dfrac{a}{c}$ lorsque $c \neq 0$ et $f(\infty) = \infty$ sinon.

Propriété. *L'application naturelle $\phi : \mathrm{GL}_2(k) \longrightarrow \mathrm{PGL}_2(k)$, qui à une matrice M associe l'homographie correspondante, est un morphisme de groupes.*

En effet, soient $A, B \in \mathrm{GL}_2(k)$. Écrivons :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

Un simple calcul montre que, pour tout $x \in \widehat{k}$, on a :

$$(\phi(A) \circ \phi(B))(x) = \frac{\left(aa' + bc'\right)x + \left(ab' + bd'\right)}{\left(a'c + c'd\right)x + \left(b'c + dd'\right)} = \phi(AB)(x)$$

1.3.2 Étude fonctionnelle du groupe $\mathrm{GL}_3(\mathbb{F}_2)$

On commence par considérer le corps $\mathbb{F}_8$ comme le quotient $\mathbb{F}_2[X]/\left(X^3 + X + 1\right)$, où $X^3 + X + 1$ est irréductible[3] sur $\mathbb{F}_2[X]$. Le groupe multiplicatif $\mathbb{F}_8^\times$ est d'ordre $8 - 1 = 7$ qui est premier, il est donc cyclique et engendré par n'importe quel élément non trivial.

Choisissons un générateur de $\mathbb{F}_8^\times$, par exemple $x = X \mod \left(X^3 + X + 1\right)$. Le corps $\mathbb{F}_8$ est alors un $\mathbb{F}_2$ espace vectoriel de dimension 3 dont une base est donnée par $\mathfrak{b} \overset{\text{def}}{=} \left(1, x, x^2\right)$.

3. Voir (♥) page 3.

On considère l'application :

$$\begin{array}{ccc} \mathrm{GL}(\mathbb{F}_8) & \longrightarrow & \mathrm{GL}_3(\mathbb{F}_2) \\ f & \longmapsto & \mathrm{Mat}(f, \mathfrak{b}) \end{array}$$

Il est loisible de constater que cette application est un isomorphisme de groupes puisque pour tout $f, g \in \mathrm{GL}(\mathbb{F}_8)$ on a $\mathrm{Mat}(f \circ g, \mathfrak{b}) = \mathrm{Mat}(f, \mathfrak{b})\,\mathrm{Mat}(g, \mathfrak{b})$; et cette application est une bijection : à une base fixée, une matrice de $\mathrm{GL}_3(\mathbb{F}_2)$ représente un unique endomorphisme de $\mathscr{L}\left(\mathbb{F}_2^3\right) \simeq \mathscr{L}(\mathbb{F}_8)$, l'application considérée est donc injective, et les groupes $\mathrm{GL}(\mathbb{F}_8)$ et $\mathrm{GL}_3(\mathbb{F}_2)$ ont le même ordre.

Dorénavant, on identifiera donc les groupes $\mathrm{GL}(\mathbb{F}_8)$ et $\mathrm{GL}_3(\mathbb{F}_2)$.

On cherche désormais un système de générateurs de $\mathrm{GL}_3(\mathbb{F}_2)$.[3]

En caractéristique 2, on a $\mathrm{GL}_3(\mathbb{F}_2) = \mathrm{SL}_3(\mathbb{F}_2)$.

En effet, tout élément de $\mathrm{GL}_3(\mathbb{F}_2)$ admet son déterminant dans $\mathbb{F}_2^\times = \{1\}$, donc c'est également un élément de $\mathrm{SL}_3(\mathbb{F}_2)$. Or $\mathrm{SL}_3(\mathbb{F}_2)$ est engendré par les transvections [4], et les transvections sont de la forme [5] $T_{ij}(1)$ avec $i, j \in [\![1, 3]\!]$ et $i \neq j$, puisque $\mathbb{F}_2^\times = \{1\}$.

Remarque. *On peut également se souvenir que $\mathrm{GL}_3(\mathbb{F}_2)$ est engendré par les transvections et au plus une dilatation, mais il n'y a pas de dilatations en caractéristique 2.*

Montrons que l'on peut obtenir toutes les transvections à partir d'une seule, disons $T_{23}(1) = M_2$, et les matrices de permutations $\left(S_\sigma\right)_{\sigma \in \mathfrak{S}_3}$. Rappelons ce que sont les matrices de permutation.

Définition 1.3.7 (Matrice de permutation)**.** *Soit $n \in \mathbb{N}^*$. Si $\sigma \in \mathfrak{S}_n$, on appelle* matrice de permutation associée à σ *la matrice $P_\sigma \in \mathcal{M}_n(k)$ telle que :*

$$\forall i, j \in [\![1, n]\!], \quad \left[P_\sigma\right]_{ij} = \delta_{i\sigma(j)}$$

où δ désigne le symbole de Kronecker.

Propriétés.

- *Si $\sigma \in \mathfrak{S}_n$, P_σ est une matrice inversible. On peut donc voir les matrices de permutation comme des éléments du groupe linéaire $\mathrm{GL}_n(k)$, d'où la remarque suivante :*
- *L'application naturelle $\mathfrak{S}_n \longrightarrow \mathrm{GL}_n(k)$ qui a une permutation associe la matrice qui lui est associée, est un morphisme de groupes.*

  On peut en effet vérifier que si $\sigma, \tau \in \mathfrak{S}_n$, alors pour tout $i, j \in [\![1, n]\!]$, on a :

$$\left[P_\sigma P_\tau\right]_{ij} = \sum_{l=1}^{n} \left[P_\sigma\right]_{il} \left[P_\tau\right]_{lj} = [P_\sigma]_{i\tau(j)} = \delta_{i\,\sigma\circ\tau(j)} = \left[P_{\sigma\tau}\right]_{ij}$$

On examine ces matrices de permutations d'un peu plus près dans un cadre général. Pour ce faire on se replace dans $E = k^n$ et on prend $\sigma \in \mathfrak{S}_n$ et $A = \left(a_{ij}\right)_{i,j \in [\![1,n]\!]} \in \mathcal{M}_n(k)$. Soient $i, j \in [\![1, n]\!]$. On calcule :

$$\left[AP_\sigma\right]_{ij} = \sum_{l=1}^{n} a_{il}\delta_{l\sigma(j)} = a_{i\sigma(j)}$$

$$\left[P_\sigma A\right]_{ij} = \sum_{l=1}^{n} \delta_{i\sigma(l)}a_{lj} = a_{\sigma(i)j}$$

On constate ainsi que multiplier A à droite (respectivement à gauche) par P_σ revient à permuter les colonnes (respectivement les lignes) de A : la colonne j (respectivement la ligne i) se retrouve en position $\sigma(j)$ (respectivement $\sigma(i)$).

4. Voir proposition 1.2.3.
5. Voir page 13.

Revenons-en à $\mathrm{GL}_3(\mathbb{F}_2)$: si $T_{ij}(1)$ est une transvection, alors on a par ce qui précède qu'on peut multiplier à gauche et à droite par des matrices de permutation P_σ et P_τ de telle sorte à avoir :

$$T_{ij}(1) = P_\sigma T_{23}(1) P_\tau$$

Mais $\mathfrak{S}_3$ est engendré par les transpositions, et on a $(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$, donc $\mathfrak{S}_3 = \langle (1\ 2), (2\ 3) \rangle$.

En utilisant la formule de multiplication des matrices de permutation (le caractère de morphismes de groupes décrit dans la propriété de la page 20), on peut écrire n'importe quelle transvection $T_{ij}(1)$ comme un produit faisant intervenir $P_{(1\ 2)}$, $P_{(2\ 3)}$ et $T_{23}(1) = M_2$. Et on en déduit que :

$$\mathrm{GL}_3(\mathbb{F}_2) = \left\langle M_2, P_{(1\ 2)}, P_{(2\ 3)} \right\rangle$$

À partir de ceci, on trouve un nouveau système de générateurs en considérant les matrices suivantes :

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

En effet, on vérifie par le calcul que :

$$M_2 = A_1 A_3 \quad P_{(1\ 2)} = A_2^2 A_1 A_2^3 A_3 \quad P_{(1\ 2)} = A_1$$

Ainsi on a :

Propriété.

$$\mathrm{GL}_3(\mathbb{F}_2) = \langle A_1, A_2, A_3 \rangle$$

1.3.3 Un portrait de $\mathrm{PSL}_2(\mathbb{F}_7)$

Dans la suite, on prend $k = \mathbb{F}_7$ et $G = \mathrm{SL}_2(\mathbb{F}_2)$ et on regarde $\phi : \mathrm{SL}_2(\mathbb{F}_7) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_7)$.

On fixe $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F_7)$.

On a $\ker(\phi) = \left\{ \pm \mathrm{I}_2 \right\}$.

— « Sens $\subseteq$ » : supposons que $\phi(A) = \mathrm{id}_{\widehat{\mathbb{F}_7}}$, c'est-à-dire que pour tout $x \in \widehat{\mathbb{F}_7}$:

$$\frac{ax+b}{cx+d} = x \qquad \text{i.e.} \qquad cx^2 + (d-a)\,x - b = 0$$

On remarque que cette dernière égalité peut être vue comme l'évaluation en x d'un polynôme P de degré au plus 2 sur le corps $\mathbb{F}_7$ et que l'équation polynomiale associée est constamment nulle. Puisque P a au moins $7 > \deg P$ racines, on a que $P = 0$.

Ainsi les coefficients de l'égalité précédentes sont nuls, autrement dit $A = \lambda \mathrm{I}_2$ pour un certain $\lambda \in \mathbb{F}_7$.

Mais alors $1 = \det(A) = \lambda^2$, ainsi $\lambda = \pm 1$, d'où $\ker(\phi) \subseteq \left\{ \pm \mathrm{I}_2 \right\}$.

— « Sens $\supseteq$ » : on constate aisément que $\phi\left(\pm \mathrm{I}_2\right) = \mathrm{I}_2$.

On en déduit le fait suivant :

Propriété. *En posant $H(\mathrm{SL}_2(\mathbb{F}_7))$ l'ensemble des homographies de $\mathrm{SL}_2(\mathbb{F}_7)$, on a :*

$$\mathrm{PSL}_2(\mathbb{F}_7) = \mathrm{SL}_2(\mathbb{F}_7) \Big/ \left\{ \pm \mathrm{I}_2 \right\} \simeq H(\mathrm{SL}_2(\mathbb{F}_7))$$

Cette relation est une conséquence premier théorème d'isomorphisme.

On veut désormais trouver des générateurs de $\mathrm{PSL}_2(\mathbb{F}_7)$ grâce à cette identification.[3]

On considère les trois homographies suivantes :

- La « réflexion » : $r : x \longmapsto -\dfrac{1}{x}$
- La « translation » : $t : x \longmapsto x + 1$
- Le « doublement » : $\delta : x \longmapsto 2x$

Remarque. *On peut représenter les trois homographies précédentes avec des matrices de* $\mathrm{SL}_2(\mathbb{F}_7)$. *Pour les deux premières, il est clair que l'on peut choisir les deux matrices*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

qui sont bien des éléments de $\mathrm{SL}_2(\mathbb{F}_7)$. *Pour la troisième, il faut être un peut plus astucieux et remarquer que* $2 \cdot 5 = 3$ *dans* $\mathbb{F}_7$, *donc que* $2 = \frac{3}{5}$. *Ainsi* $\delta : x \longmapsto \frac{3}{5}x$ *que l'on peut représenter par la matrice*

$$\begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$$

qui est de déterminant 1 *dans* $\mathrm{GL}_2(\mathbb{F}_7)$.

On veut montrer que, étant donnée une homographie f à coefficients dans $\mathrm{SL}_2(\mathbb{F}_7)$, $f \in \langle r, t, \delta \rangle$. Pour ce faire, on prend f une homographie représentée par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_7)$.

Si $c = 0$: on doit avoir $d = a^{-1}$, et pour tout $x \in \widehat{\mathbb{F}_7}$, $f(x)$ peut se réécrire $f(x) = a^2x + ab$. Sachant que les carrés non nuls de $\mathbb{F}_7$ sont $1, 2$ et 4, il existe $i \in [\![0, 2]\!]$ tel que $a^2 = 2^i$, et alors on peut écrire :

$$f = t^{ab} \circ \delta^i$$

Si $c \neq 0$: on prend $x \in \widehat{\mathbb{F}_7}$. Il vient alors :

$$f(x) = \frac{ax + b}{cx + d} = \frac{a(cx + d) + bc - ad}{c(cx + d)} = \frac{a}{c} + \frac{bc - ad}{c(cx + d)} = \left(ac^{-1}\right) - \frac{1}{c^2x + cd}$$

Comme précédemment, on écrit $c^2 = 2^i$ avec $i \in [\![0, 2]\!]$, et il vient alors :

$$f = t^{ac^{-1}} \circ r \circ t^{cd} \circ \delta^i$$

Toute homographie de $H(\mathrm{SL}_2(\mathbb{F}_7))$ peut donc s'écrire comme une composée des trois homographies r, t et δ, ainsi nous avons un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_7) \simeq H(\mathrm{SL}_2(\mathbb{F}_7)) = \langle r, t, \delta \rangle$: on a trouvé un système de générateur à $\mathrm{PSL}_2(\mathbb{F}_7)$.

$$\mathrm{PSL}_2(\mathbb{F}_7) = \left\langle \overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}, \overline{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}, \overline{\begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}} \right\rangle$$

où $\overline{M}$ désigne la classe de $M \in \mathrm{SL}_2\left(\mathbb{F}_7\right)$ dans $\mathrm{PSL}_2\left(\mathbb{F}_7\right)$.

1.3.4 L'isomorphisme $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$

On définit, pour x un générateur[6] de $\mathbb{F}_8^\times$, $x^\infty \overset{\text{def}}{=} 0$. On fait alors l'identification $\mathbb{F}_8 = \left\{ x^m \mid m \in \widehat{\mathbb{F}_7} \right\}$. On considère alors l'application :

$$T = \left\{ \begin{array}{ccc} H(\mathrm{SL}_2(\mathbb{F}_7)) & \longrightarrow & \mathrm{GL}(\mathbb{F}_8) \\ f & \longmapsto & T_f \end{array} \right.$$

où T_f est définie par $T_f : x^m \longmapsto x^{f(m)} + x^{f(\infty)}$. Vérifions que T_f est bien un automorphisme de $\mathbb{F}_8$, pour f une homographie.

Remarque. *Pourquoi devons-nous ajouter* $x^{f(\infty)}$ *? C'est pour avoir une chance d'avoir* $F_f(0) = 0$. *En effet, on remarque que nous sommes en caractéristique* 2, *donc on a :*

$$T_f(0) = T_f(x^\infty) = x^{f(\infty)} + x^{f(\infty)} = 0$$

C'est un premier pas vers la linéarité !

Pour montrer que les T_f sont bien des éléments de $\mathrm{GL}(\mathbb{F}_8)$, on commence par regarder ce qu'il se passe pour $f \in \{r, t, \delta\}$ les générateurs de $H(\mathrm{SL}_2(\mathbb{F}_7))$[7].

6. Voir comment choisir un générateur à la page 19.
7. Voir la partie précédente.

• Cas de T_r : on commence par écrire ce que fait r en faisant correspondre chaque élément avec son image par r sous la forme du tableau suivant :

$$r = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ \infty & 6 & 3 & 2 & 5 & 4 & 1 & 0 \end{pmatrix}$$

Dans $\mathbb{F}_8$ on a $x^3 + x + 1 = 0$, ainsi :

$$x^3 = x + 1 \quad x^4 = x^2 + x \quad x^5 = x^2 + x + 1 \quad x^6 = x^2 + 1$$

On représente chaque élément de $\mathbb{F}_8$ sous la forme $b_2x^2 + b_1x + b_0$, que l'on écrira pour simplifier $b_2b_1b_0$, il vient ainsi :

$$x^0 = 001 \quad x^1 = 010 \quad x^2 = 100 \quad x^3 = 011 \quad x^4 = 110 \quad x^5 = 111 \quad x^6 = 101 \quad x^\infty = 000$$

On écrit alors T_r de la sorte :

$$T_r = \begin{pmatrix} 001 & 010 & 100 & 011 & 110 & 111 & 101 & 000 \\ 001 & 100 & 010 & 101 & 110 & 111 & 011 & 000 \end{pmatrix}$$

On remarque que T_r ne fait qu'échanger les deux premiers « chiffres » d'un élément, autrement dit elle envoie le vecteur x^2 sur x et réciproquement, et laisse inchangé le vecteur 1 ; autrement dit T_r est bien linéaire et se représente dans la base $\mathfrak{b} \overset{\text{def}}{=} (1, x, x^2)$ par :

$$\mathrm{Mat}(T_r, \mathfrak{b}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A_1$$

Cette matrice est inversible, donc $T_r \in \mathrm{GL}(\mathbb{F}_8)$.

• Cas de T_t : pour $m \in \widehat{\mathbb{F}_7}$, $m \neq \infty$, on a :

$$T_t(x^m) = x^{t(m)} + x^{t(\infty)} = x^{m+1} + x^\infty = x\,(x^m)$$

Ainsi T_t est la multiplication par x dans $\mathbb{F}_8$, ainsi T_f est bien linéaire : si $m_1, m_2 \in \widehat{\mathbb{F}_7}$, on a :

$$T_t\,(x^{m_1} + x^{m_2}) = x\,(x^{m_1} + x^{m_2}) = x\,(x^{m_1}) + x\,(x^{m_2}) = T_t\,(x^{m_1}) + T_t\,(x^{m_2})$$

De plus, T_t est clairement inversible : il suffit de considérer la multiplication $x^{-1} = x^6$ dans $\mathbb{F}_8$ pour avoir un excellent candidat d'inverse pour T_t ! Encore une fois, écrivons la matrice de T_t dans la base $\mathfrak{b}$:
Le vecteur 1 est envoyé sur x, qui est lui-même envoyé sur x^2, et x^2 est envoyé sur $x^3 = x + 1$, ainsi on a :

$$\mathrm{Mat}(T_t, \mathfrak{b}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A_2$$

• Cas de T_δ : pour $m \in \widehat{\mathbb{F}_7}$, $m \neq \infty$, on a :

$$T_\delta(x^m) = x^{t(m)} + x^{t(\infty)} = x^{2m} + x^\infty = (x^m)^2$$

Ainsi T_δ est l'élévation au carré dans $\mathbb{F}_8$. Cette application est bien linéaire puisque nous sommes en caractéristique 2, et donc nous avons $(u + v)^2 = u^2 + v^2$. Étant linéaire, on peut encore une fois écrire la matrice de T_δ dans la base $\mathfrak{b}$:
Le vecteur 1 reste sur 1, le vecteur x est envoyé sur x^2, et enfin x^2 est envoyé sur $x^4 = x^2 + x$, d'où :

$$\mathrm{Mat}(T_t, \mathfrak{b}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = A_3$$

Cette matrice étant inversible, on a bien $T_\delta \in \mathrm{GL}(\mathbb{F}_8)$.

Il nous faut désormais regarder le cas général. Pour cela nous aurons besoin d'un lemme :

Lemme 1.3.8. *Soient f, g des homographies de $H(\mathrm{SL}_2(\mathbb{F}_7))$ telles que T_f et T_g soient des éléments de $\mathrm{GL}(\mathbb{F}_8)$. Alors on a :*

$$T_{f\circ g} = T_f \circ T_g$$

Démonstration. Soit $m \in \widehat{\mathbb{F}_7}$. On a alors :

$$\begin{aligned}\left(T_f \circ T_g\right)(x^m) &= T_f\left(x^{g(m)} + x^{g(\infty)}\right) \\ &= T_f\left(x^{g(m)}\right) + T_f\left(x^{g(\infty)}\right) && \text{(Linéarité de } T_f\text{)} \\ &= x^{f(g(m))} + x^{f(\infty)} + x^{f(g(\infty))} + x^{f(\infty)} \\ &= x^{f\circ g(m)} + x^{f\circ g(\infty)} \\ &= T_{f\circ g}(x^m)\end{aligned}$$

D'où le résultat voulu. □

Ce lemme va nous être d'être une grande aide pour montrer que T est un isomorphisme de groupes $H(\mathrm{SL}_2(\mathbb{F}_7)) \longrightarrow \mathrm{GL}(\mathbb{F}_8)$.

En effet, on utilise à présent le fait que tout élément de $H(\mathrm{SL}_2(\mathbb{F}_7))$ est une composition de r, t et δ, qui sont des éléments de $\mathrm{GL}(\mathbb{F}_8)$ d'après notre étude préliminaire. Le lemme précédent nous donne alors que :

$$\forall f \in H(\mathrm{SL}_2(\mathbb{F}_7)), \quad f = \prod_{f_i \in \{r,t,\delta\}} f_i \quad \Longrightarrow \quad T_f = \prod_{f_i \in \{r,t,\delta\}} T_{f_i} \in \mathrm{GL}(\mathbb{F}_8)$$

où le produit désigne le produit respectif des groupes $H(\mathrm{SL}_2(\mathbb{F}_7))$ et $\mathrm{GL}(\mathbb{F}_8)$, c'est-à-dire la composition d'applications.

Cela nous donne que T est bien à valeur dans $\mathrm{GL}(\mathbb{F}_8)$. Mais surtout le *lemme 1.3.8* nous donne que T est bien un morphisme de groupes.

Il ne reste plus qu'à montrer que T est bien une bijection.

De tout ce qui a été dit précédemment, nous en déduisons que l'image de T contient T_r, T_t et T_δ, et sa qualité de morphisme de groupes nous donne que l'image de T contient [8] $\langle A_1, A_2, A_3\rangle = \mathrm{GL}_3(\mathbb{F}_2)$ par la propriété de la page 21. Ainsi T est surjective, et $H(\mathrm{SL}_2(\mathbb{F}_7))$ et $\mathrm{GL}_3(\mathbb{F}_2)$ ont tous deux 168 éléments, ainsi $H(\mathrm{SL}_2(\mathbb{F}_7)) \simeq \mathrm{GL}_3(\mathbb{F}_2)$.

Cela nous donne que :

Théorème 1.3.9. *Les groupes* $\mathrm{GL}_3(\mathbb{F}_2)$ *et* $\mathrm{PSL}_2(\mathbb{F}_7)$ *sont isomorphes.*

Démonstration. Par une propriété précédente [9], on avait déjà $\mathrm{PSL}_2(\mathbb{F}_7) \simeq H(\mathrm{SL}_2(\mathbb{F}_7))$ l'ensemble des homographies de $\mathrm{SL}_2(\mathbb{F}_7)$, qui est lui-même isomorphe à $\mathrm{GL}_3(\mathbb{F}_2)$ par ce qui précède. □

1.4 Complément : autre point de vue sur $\mathrm{GL}_3(\mathbb{F}_2)$

L'un des objectifs de cette partie était d'exhiber un groupe simple d'ordre 168, et nous avons jeté notre dévolu sur $\mathrm{GL}_3(\mathbb{F}_2)$. Il est en effet assez facile de montrer que ce groupe est d'ordre 168, mais c'est en revanche plus compliqué d'en montrer la simplicité.

Pour ce dernier point, nous aurions pu ajouter un nouvel isomorphisme à notre collection :

Propriété (Un autre isomorphisme)**.** *On a* $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_3(\mathbb{F}_2)$.

En effet, nous sommes en caractéristique 2 donc le déterminant d'un élément de $\mathrm{GL}_3(\mathbb{F}_2)$ ne peut valoir que 1, ce qui nous donne que $\mathrm{GL}_3(\mathbb{F}_2) = \mathrm{SL}_3(\mathbb{F}_2)$.
Le centre de $\mathrm{SL}_3(\mathbb{F}_2)$ est formé des homothéties de rapport $\lambda \in \mathbb{F}_2^\times = \{1\}$, donc $Z(\mathrm{SL}_3(\mathbb{F}_2))$ ne contient que l'identité.
Or $\mathrm{PSL}_3(\mathbb{F}_2)$ est le quotient de $\mathrm{SL}_3(\mathbb{F}_2)$ par son centre, d'où $\mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{SL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2)$.

Le *théorème 1.2.9* nous donne alors que $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_3(\mathbb{F}_2)$ est simple.

8. On identifie ici un élément $f \in \mathrm{GL}(\mathbb{F}_8)$ à sa matrice dans la base $\mathfrak{b} = (1, x, x^2)$, qui est bien un élément de $\mathrm{GL}_3(\mathbb{F}_2)$. Ainsi quand j'écris que l'image de T « contient » A_1, A_2, A_3, c'est après avoir fait cette identification.
9. Voir la propriété de la page 21.

2 Unicité d'un groupe simple d'ordre 168

De but de cette partie est de montrer qu'il existe un unique groupe simple d'ordre 168.

2.1 Quelques outils pour l'étude de la structure des groupes finis

Dans cette sous-partie nous établirons une petite liste non exhaustive de différents théorèmes qui nous seront utiles pour étudier la structure des groupes finis.

2.1.1 Les théorèmes de Sylow

Nous commençons par un incontournable de la théorie des groupes finis, le(s) théorème(s) de Sylow. Originellement publiés comme un ensemble de trois théorèmes, on y fait aujourd'hui parfois référence comme **le** théorème de Sylow, aussi j'utiliserai tantôt le singulier ou tantôt le pluriel pour parler de(s) théorème(s) de Sylow.

Tout d'abord nous introduisons une notion qui nous sera très utile par la suite, à savoir :

Définition 2.1.1 (p-Sylow)**.** *Soit G un groupe fini d'ordre $p^\alpha q$ où q est un entier, p un nombre premier ne divisant pas q et $\alpha \in \mathbb{N}^*$. On appelle p-*Sylow de G *tout sous-groupe de G d'ordre p^α.*

Définition 2.1.2 (Normalisateur)**.** *Soit G un groupe et X une partie de G. On appelle* normalisateur de X dans G *le sous-groupe de G défini par :*

$$N_G(X) = \left\{ g \in G \mid gXg^{-1} = X \right\}$$

Propriétés.

- *Si H est un sous-groupe de G, alors $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est distingué. En particulier, on a que $N_G(H) = G$ si et seulement si $H \lhd G$.*
- *Pour $X \subseteq G$, le centralisateur (voir la* définition 1.1.9*) de X est distingué dans $N_G(X)$.*

Nous serons amenés à utiliser des outils indispensables dans l'étude de la structure des groupe finis : les théorèmes de Sylow, que nous rappelons ici :

Théorème 2.1.3 (Sylow)**.** *Soit G un groupe fini d'ordre $p^\alpha q$, où p est un nombre premier, q est un entier premier avec p, et $\alpha \in \mathbb{N}^*$. Alors nous avons :*

1. *Le groupe G admet des p-Sylow.*
2. *Si P et Q sont deux p-Sylow de G, alors il existe $g \in G$ tel que $P = gQg^{-1}$. En particulier tous les p-Sylow de G sont conjugués entre eux.*
3. *Si H est un p-sous-groupe de G, alors il existe P un p-Sylow de G tel que $H \subseteq P$.*
4. *Si n_p désigne le nombre de p-Sylow de G, alors on a :*
   (a) *Soit P un p-Sylow de G. Alors $n_p = [G : N_G(P)]$.*
   (b) *En particulier, $n_p \mid m$.*
   (c) *$n_p \equiv 1\,[p]$.*

Notation. *Si G est un groupe fini d'ordre $p^\alpha q$, nous noterons $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylow de G.*
Pour ne pas alourdir les notations dans les prochaines parties, je me contenterai souvent de Syl_p sans préciser le groupe d'étude s'il est implicite que nous étudions un groupe G donné, typiquement quand nous aurons posé G un groupe simple d'ordre 168*.*
Le premier point du théorème de Sylow nous donne que $\mathrm{Syl}_p(G)$ est un ensemble non vide.

Corollaire 2.1.4. *Soit G un groupe fini d'ordre $p^\alpha q$, et soit $P \in \mathrm{Syl}_p$. Nous avons alors que $P \lhd G$ si et seulement si P est l'unique p-Sylow de G.*

Démonstration. C'est une conséquence directe du deuxième point du théorème de Sylow : si P est distingué dans G, alors $gPg^{-1} = P$ pour tout g, donc P est l'unique p-Sylow de G. Réciproquement, si $n_p = 1$, puisque tous les p-Sylow de G sont conjugués entre eux, cela donne que P est stable par tout automorphisme intérieur, et donc est distingué dans G. □

2.1.2 Indices de sous-groupes

Afin d'étudier les sous-groupes d'un groupe simple, nous énonçons ici un théorème à propos des indices des sous-groupes qui nous donnera les conditions nécessaires de simplicité d'un groupe fini.

Théorème 2.1.5 (de l'indice)**.** *Soit G un groupe admettant un sous-groupe strict H d'indice fini m.*
Si $|G| \nmid m!$, alors G contient un sous-groupe propre K distingué dans G. En particulier, G n'est pas simple.

Démonstration. On pose $X \overset{\text{def}}{=} G/H$, et on considère l'action de G sur X par translation à gauche. Cette action est transitive et induit un morphisme :

$$\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(X) \\ g & \longmapsto & \sigma_g : \overline{x} \longmapsto \overline{gx} \end{array} \right.$$

Ce morphisme est non-trivial puisque l'action par translation est transitive, et son noyau $\ker \varphi$ est alors un sous-groupe strict et distingué de G. On pose $K \overset{\text{def}}{=} \ker \varphi$.
Le premier théorème d'isomorphisme nous donne que $G/K \simeq \operatorname{im} \varphi \leqslant \mathfrak{S}(X)$. Or X est un ensemble fini de cardinal $[G : H] = m$, donc $\mathfrak{S}(X)$ est d'ordre $m!$; le sous-groupe K est donc d'indice fini dans G et cet indice est l'ordre de $\operatorname{im} \varphi$ qui divise donc $m!$.
Supposons que $|G| \nmid m!$. Alors $K \neq \{1_G\}$, sinon K serait un sous-groupe d'indice $|G|$ qui diviserait alors $m!$; mais nous avions aussi vu que $K \neq G$, ainsi K est un sous-groupe propre et distingué de G.
En bonus, le groupe G ne peut donc pas être simple. □

Corollaire 2.1.6. *Soit G un groupe fini simple, et soit $N = \min_{m \in \mathbb{N}^*} \{|G| \mid m!\}$. Alors, pour tout sous-groupe H de G, on a $[G : H] \geqslant N$.*

Démonstration. Notons $n \overset{\text{def}}{=} |G|$.
Il suffit de montrer que N est bien défini. En effet, par contraposée du *théorème 2.1.5*, tout sous-groupe de G d'indice m vérifie que $n \mid m!$ et donc $m \geqslant N$ par définition de N.
Montrons que n est bien défini. Posons $E \overset{\text{def}}{=} \left\{ m \in \mathbb{N}^* \;\middle|\; n \mid m! \right\}$. Cet ensemble est une partie de $\mathbb{N}$; et puisque n divise $n!$ et que $n \in \mathbb{N}^*$, $n \in E$. Ainsi $E \neq \varnothing$, E est donc une partie non vide de $\mathbb{N}$, E admet donc un plus petit élément, et N est donc bien défini. □

2.1.3 Action doublement transitive

On introduit ici une nouvelle notion d'action de groupe qui nous sera utile dans l'étude de notre groupe simple d'ordre 168.

Définition 2.1.7 (Action doublement transitive)**.** *Soit G un groupe opérant sur un ensemble X. On dit que G* agit doublement transitivement sur X *si pour tous couples $(x_1, x_2), (y_1, y_2) \in X^2$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$, il existe $g \in G$ tel que $g \cdot x_1 = y_1$ et $g \cdot x_2 = y_2$.*

Remarque. *Nous avons déjà rencontré un exemple d'action doublement transitive dans le lemme intermédiaire de la* page 15 *dans la preuve de la simplicité des espaces projectifs (voir* Théorème 1.2.9*).*

Dans la suite, on se donne G un groupe agissant sur un ensemble X, et on fixe une fois pour toute $x \in X$, et on note $H \overset{\text{def}}{=} \operatorname{Stab}_G(x)$.

On veut donner une caractérisation du fait que G agisse doublement transitivement sur X.

Proposition 2.1.8. *Avec les notations précédentes, nous avons que G agit doublement transitivement sur X si et seulement si G agit transitivement sur X et H agit transitivement sur $X \setminus \{x\}$.*

Démonstration. Montrons le résultat par double implication.

- ($\Longrightarrow$) Il est évident que G agit transitivement sur G : ce qui est vérifié pour deux paires d'éléments de X est aussi vérifié pour une seule paire. De plus, si $x_1, y_1 \in X$ sont deux éléments distincts de x, alors on peut appliquer la définition de l'action doublement transitive aux couples (x_1, x) et (y_1, x), et il existe alors $h \in G$ tel que $h \cdot x_1 = y_1$ et $h \cdot x = x$, donc $h \in \mathrm{Stab}_G(x)$, d'où $h \in H$. Le groupe H agit donc transitivement sur $X \setminus \{x\}$.
- ($\Longleftarrow$) Supposons que G agisse transitivement sur X et que H agisse transitivement sur $X \setminus \{x\}$.
  Soit $z \in X$. Commençons par montrer que $\mathrm{Stab}_G(z)$ agit transitivement sur $X \setminus \{z\}$.
  Puisque G agit transitivement sur X, il existe $g_0 \in G$ tel que $z = g_0 \cdot x$.
  Si $z_1, z_2 \in X \setminus \{z\}$, alors $g_0^{-1} z_1$ et $g_0^{-1} z_2$ sont distincts de x. Mais H agit transitivement sur $X \setminus \{x\}$, donc il existe $h \in H$ tel que $\left(h g_0^{-1}\right) \cdot z_1 = g_0^{-1} z_2$, et en posant $g \overset{\text{def}}{=} g_0 h g_0^{-1}$, il vient que $g \cdot z_1 = z_2$.
  Nous devons donc montrer que g stabilise z, ce dont on s'aperçoit en remarquant que $g \cdot z = g_0 h \cdot \left(g_0^{-1} \cdot z\right) = g_0 h \cdot x$. Mais H agit transitivement sur $X \setminus \{x\}$, donc $h \cdot x = x$ nécessairement, ce qui nous donne que $g \cdot z = g_0 \cdot x = z$, donc $g \in \mathrm{Stab}_G(z)$.
  Ainsi pour tout $z \in X$, $\mathrm{Stab}_G(z)$ agit transitivement sur $X \setminus \{z\}$.

  Montrons que G agit doublement transitivement : si $(x_1, x_2), (y_1, y_2) \in X^2$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$, alors par transitivité de G, il existe $g \in G$ tel que $y_2 = g \cdot x_2$. Par hypothèse, nous avons $y_1 \neq y_2$ donc $g^{-1} \cdot y_1 \neq g^{-1} \cdot y_2 = x_2$. Ainsi, x_1 et $g^{-1} \cdot y_1$ sont tous les deux distincts de x_2, et on sait par la première partie de la preuve que $\mathrm{Stab}_G(x_2)$ agit transitivement sur $X \setminus \{x_2\}$, il existe donc $h \in \mathrm{Stab}_G(x_2)$ tel que $h \cdot x_1 = g^{-1} \cdot y_1$, c'est-à-dire que $(gh)x_1 = y_1$. De plus, $(gh) \cdot x_2 = g \cdot (hx_2) = g x_2 = y_2$, on prend donc gh qui permet de doublement transiter de (x_1, x_2) vers (y_1, y_2), ce qui montre que G est doublement transitif.

  □

Cette notion nous permet de montrer un résultat qui nous aidera plus tard à montrer qu'une partie donnée du groupe simple d'ordre 168 est génératrice.

Théorème 2.1.9. *Soit G un groupe agissant doublement transitivement sur un ensemble X, et soit $x \in X$. Comme ce qui a été fait précédemment, on pose $H \overset{\text{def}}{=} \mathrm{Stab}_G(x)$.*
Alors H est un sous-groupe propre maximal.

Démonstration. Soit $g \in G \setminus H$, et soit K un sous-groupe de G contenant H et $\{g\}$.
Soit $g_0 \in G \setminus H$. On pose $y = g \cdot x$ et $y_0 = g_0 \cdot x$. Puisque $g, g_0 \in G \setminus H$, les éléments g et g_0 ne peuvent par définition par stabiliser x sous l'action de G, et donc $y, y_0 \in X \setminus \{x\}$.
Par la propriété précédente, H agit transitivement sur $X \setminus \{x\}$, donc il existe $h \in H$ tel que $h \cdot y = y_0$, c'est-à-dire que $(hg) \cdot x = g_0 \cdot x$, donc $h_0 \overset{\text{def}}{=} g_0^{-1} h g$ stabilise x, d'où $g_0 = h g h_0^{-1} \in HgH$.
On a donc réussi à écrire tout élément de $G \setminus H$ comme un élément de HgH, donc $G = H \cup HgH$. Puisque K contient à la fois H et $\{g\}$, K contient HgH et H, d'où $K = G$. □

Corollaire 2.1.10. *Soit G un groupe agissant doublement transitivement sur X.*
Si on prend $x \in X$ et $g \in G \setminus \mathrm{Stab}_G(x)$, alors $G = \langle \mathrm{Stab}_G(x), g \rangle$.

2.1.4 Lemme N/C

On présente un résultat tiré de *An Introduction to the Theory of Groups*[6] qui permet de nous renseigner sur la structure des normalisateurs des éléments d'un groupe.

Lemme 2.1.11 (Lemme N/C)**.** *Soit G un groupe et H un sous-groupe de G. Alors le centralisateur[10] $C_G(H)$ est un sous-groupe distingué du normalisateur $N_G(H)$.*

De plus, le groupe quotient $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de Aut (H).

Démonstration. Pour tout $g \in G$, on note γ_g l'automorphisme intérieur de conjugaison par g. On considère alors l'application :

$$\varphi : \left\{ \begin{array}{ccc} N_G(H) & \longrightarrow & \mathrm{Aut}(H) \\ h & \longmapsto & \gamma_{h|H} \end{array} \right.$$

Les $\gamma_{h|H}$ pour $h \in N_G(H)$ sont en effet des automorphismes de H par définition du normalisateur de H. Il est de plus immédiat que φ est un morphisme de groupes : si $h, h' \in N_G(H)$, alors $\varphi\left(hh'\right)$ est l'application de conjugaison par hh', c'est-à-dire l'application qui à $a \in H$ associe $hh'ah'^{-1}h^{-1} = \gamma_{h|H}\left(\gamma'_{h|H}(a)\right) = \gamma_{h|H} \circ \gamma_{h'|H}(a)$, ce qui nous donne que $\varphi\left(hh'\right) = \varphi(h)\,\varphi\left(h'\right)$.
On remarque alors que nous avons les équivalences :

$$\begin{aligned} a \in \ker\varphi &\iff \gamma_{a|H} = \mathrm{id}_H \\ &\iff \forall h \in H,\ aha^{-1} \in H \\ &\iff a \in C_G(H) \end{aligned}$$

Par le premier théorème d'isomorphisme, $C_G(H) = \ker\varphi \lhd N_G(H)$ et $N_G(H)/C_G(H) \simeq \mathrm{im}\,\varphi$ qui est un sous-groupe de Aut(H). □

2.2 Étude générale d'un groupe simple d'ordre 168

À partir d'ici, et sauf mention contraire, G désignera un groupe simple d'ordre 168.

2.2.1 Les 7-Sylow de G

Nous pouvons commencer notre étude de la structure de G.

Rappelons que $|G| = 168 = 2^3 \cdot 3 \cdot 7$. Par les théorèmes de Sylow, G admet des 2-Sylow, des 3-Sylow et des 7-Sylow, au nombre de n_2,n_3 et n_7 respectivement.

L'hypothèse de simplicité de G donne qu'aucun des nombres n_2, n_3 et n_7 ne vaut 1 : nous savons en effet que pour $p \in \{2,3,7\}$, tous les p-Sylow de G sont conjugués entre eux, ainsi l'existence d'un unique p-Sylow nous donnerait que ce p-Sylow est stable par tout automorphisme intérieur, et donc serait distingué dans G. Mais p n'est pas l'unique diviseur premier de $|G|$, ainsi un p-Sylow unique serait un sous-groupe strict et distingué de G, et G ne pourrait pas être simple.

Maintenant, nous pouvons regarder ce que nous donne le théorème de Sylow sur le nombre de p-Sylow de G. On a :

$$\begin{array}{llllll} n_2 \mid 3 \cdot 7 = 21 & \text{et} & n_2 \equiv 1\,[2] & \text{donc} & n_2 \in \{1, 3, 7, 21\} & \\ n_3 \mid 2^3 \cdot 7 = 56 & \text{et} & n_3 \equiv 1\,[3] & \text{donc} & n_3 \in \{1, 4, 7, 28\} & (\clubsuit) \\ n_7 \mid 2^3 \cdot 3 = 24 & \text{et} & n_7 \equiv 1\,[7] & \text{donc} & n_7 \in \{1, 8\} & \end{array}$$

Nous nous référerons souvent à cette première évaluation du nombre de p-Sylow de G.
Cela nous permet déjà de déduire la propriété suivante :

Propriétés.

- *Le groupe G admet exactement* 8 *7-Sylow.*

  C'est ce que nous pouvons déduire les théorèmes de Sylow et de la simplicité de G.
- *Le groupe G admet* 48 *éléments d'ordre* 7.

  En effet, les éléments d'ordre 7 sont tous contenus dans un des 7-Sylow, au nombre de 8, mais un 7-Sylow de G est d'ordre 7 qui est premier, il est donc cyclique et compte $7 - 1 = 6$ éléments d'ordre 7. De plus, l'intersection de deux 7-Sylow distincts est triviale : si $g \neq 1$ est dans deux 7-Sylow, alors g engendre ces deux sous-groupes qui sont donc égaux. On a donc $6 \cdot 8 = 48$ éléments d'ordre 7 dans G.

10. Le centralisateur d'une partie est défini à la *page 9*.

2.2.2 Les 3-Sylow de G

On considère l'action de G sur Syl_7 par conjugaison. Cette action induit un morphisme $\varphi : G \longrightarrow \mathfrak{S}(\mathrm{Syl}_7)$ donné par :

$$\forall g \in G, \quad \varphi(g) \overset{\text{def}}{=} \sigma_g : \left\{ \begin{array}{ccc} \mathrm{Syl}_7 & \longrightarrow & \mathrm{Syl}_7 \\ T & \longmapsto & gTg^{-1} \end{array} \right. \tag{★}$$

Ce morphisme est non-trivial puisque les 7-Sylow de G ne sont pas distingués.
Puisque $\ker(\varphi) \lhd G$ qui est simple et que φ est non-trivial, on a $\ker(\varphi) = \{1_G\}$: φ est donc injectif.
Par le premier théorème d'isomorphisme, on a donc :

$$G \simeq G/\ker(\varphi) \simeq \mathrm{im}(\varphi) \leqslant \mathfrak{S}(\mathrm{Syl}_7) \simeq \mathfrak{S}_8$$

On peut donc identifier G à un sous-groupe H de $\mathfrak{S}_8$.

Soit $g \in G$. On considère $\sigma_g = \tau_1 \cdots \tau_r$ la décomposition en cycle à support disjoints dans $\mathfrak{S}_8$. On sait que le ppcm des longueurs des cycles $(\tau_i)_{i \in [\![1,r]\!]}$ est l'ordre de g qui divise $|G| = 168$. En particulier, la longueur ℓ d'un de ces cycles divise 168 et est de longueur au plus 8, donc $\ell \in \{2, 3, 4, 6, 7, 8\}$.

Les cycles $(\tau_i)_{i \in [\![1,r]\!]}$ sont choisis à support disjoints, donc la somme des longueurs des cycles ne peut dépasser 8. Ainsi, un élément $g \in G$ est envoyé sur σ_g, qui ne peut s'écrire que comme dans le tableau ci-contre.

Cela nous donne un premier aperçu de quels sont les ordres possibles et impossibles pour un élément de G, et en particulier, on a :

Décomposition de σ_g	$\mathrm{o}(\sigma_g)$
Produit d'un 4-cycle et d'un 3-cycle	12
Unique 8-cycle	8
Unique 7-cycle	7
Unique 6-cycle	6
Produit d'un 6-cycle et d'une transposition	
Produit de deux 3-cycle et d'une transposition	
Produit d'un 3-cycle et d'une transposition	
Produit d'un 3-cycle et d'une double-transposition	
Unique 4-cycle	4
Produit de deux 4-cycles	
Produit d'un 4-cycle et d'une transposition	
Produit d'un 4-cycle et d'une double-transposition	
Unique 3-cycle	3
Produit de deux 3-cycles	
Une simple transposition	2
Une double-transposition	
Une triple-transposition	
Une quadruple-transposition	
L'identité seule	1

Propriété. *Un élément de G a un ordre d'au plus* 12.

On le voit dans la classification précédente, et cela correspond au cas où $g \in G$ est envoyé sur $\sigma_g = \tau_1\tau_2$ qui est le produit d'un 3-cycle et d'un 4-cycle.

Remarque. *Nous serons amenés plus tard à affiner cette borne sur l'ordre des éléments de G.*

On se penche désormais sur le cas des 3-Sylow, en considérant les normalisateurs des 7-Sylow de G. [4]

Lemme 2.2.1. *Soit $P \in \mathrm{Syl}_7$. Alors :*

(i) Le sous-groupe $N_G(P)$ est non-cyclique et est d'ordre 21.

(ii) Il y a exactement 14 *éléments d'ordre* 3 *dans $N_G(P)$, qui engendrent* 7 *sous-groupes distincts.*

Démonstration. Soit $P \in \mathrm{Syl}_7$ un des 7-Sylow de G.

(i) Nous avons $|N_G(P)| = \dfrac{|G|}{[G : N_G(P)]} = \dfrac{168}{8} = 21$. En particulier, $N_G(P)$ ne peut admettre d'éléments d'ordre 21 par la propriété précédente, ce n'est donc pas un sous-groupe cyclique.

(ii) Le groupe $N_G(P)$ étant d'ordre $21 = 3 \cdot 7$, le théorème de Sylow nous donne donc qu'il existe des 7-Sylow, au

nombre de m_7, qui vérifie :

$$m_7 \mid 3 \quad \text{et} \quad m_7 \equiv 1\,[7] \quad \text{donc} \quad m_7 = 1$$

En particulier, tous les éléments d'ordre 7 et l'élément d'ordre 1 sont dans T l'unique 7-Sylow de $N_G(P)$. Les ordres possibles pour un élément de $N_G(P)$ sont $1, 3, 7, \cancel{21}$ (l'ordre 21 est impossible car $N_G(P)$ n'est pas cyclique), les éléments d'ordre 3 de $N_G(P)$ sont donc les éléments de $N_G(P) \setminus T$, il y a donc $21 - 7^1 = 14$ éléments d'ordre 3 dans $N_G(P)$.

Ces éléments engendrent $\dfrac{14}{3-1} = 7$ sous-groupes d'ordre 3 puisque les 3-Sylow de $N_G(P)$ sont alors cycliques d'ordre premier.

□

On fixe $P \in \mathrm{Syl}_7$.

Lemme 2.2.2. *Le groupe P agit par conjugaison sur $\mathrm{Syl}_7 \setminus \{P\}$, et cette action est transitive.*

Démonstration. On considère l'application :

$$\begin{array}{ccc} P \times \mathrm{Syl}_7 \setminus \{P\} & \longrightarrow & \mathrm{Syl}_7 \setminus \{P\} \\ (p, T) & \longmapsto & p \cdot T \overset{\text{def}}{=} pTp^{-1} \end{array}$$

Cette application définit bien une action de P sur $\mathrm{Syl}_7 \setminus \{P\}$ par conjugaison ; en effet, pour tout $p \in P$ et $T \in \mathrm{Syl}_7 \setminus \{P\}$, on a que $pTp^{-1} \neq P$. En effet, si tel n'était pas le cas, on aurait $T \subseteq P$, donc $P = T$ par égalité des ordres, ce qui contredit nos hypothèses sur T. L'action de P sur $\mathrm{Syl}_7 \setminus \{P\}$ est donc bien définie.
Le sous-groupe P est un 7-Sylow de G, il est d'ordre $7^1 = 7$, donc pour tout $T \in \mathrm{Syl}_7 \setminus \{P\}$, on a :

$$|P| = 7 = |\mathcal{O}_T| \cdot |\,\mathrm{Stab}_P(T)|$$

En particulier, le cardinal de l'orbite de T divise T qui est premier. Ainsi, soit $\mathcal{O}_T = \mathrm{Syl}_7 \setminus \{P\}$ et l'action est transitive, soit $\mathcal{O}_T = \{T\}$ et l'action est triviale.

Supposons que l'action de P sur $\mathrm{Syl}_7 \setminus \{P\}$ soit triviale. Alors pour tout $p \in P$, on a $pTp^{-1} = T$ donc $P \subseteq N_G(T)$. En particulier, P et T sont alors deux 7-Sylow de $N_G(T)$ qui est d'ordre 21 par un calcul précédent.
En vertu du théorème de Sylow, $N_G(T)$ admet un unique 7-Sylow (voir le calcul dans la preuve du *lemme 2.2.1*), ce qui est impossible si T est choisi distinct de P.
L'action de P sur $\mathrm{Syl}_7 \setminus \{P\}$ est donc non-triviale : elle est donc nécessairement transitive. □

On fixe Q un autre 7-Sylow de G, distinct de P, et on pose $M = N_G(P) \cap N_G(Q)$.

Considérons cette fois-ci l'action de $N_G(P)$ sur Syl_7 par conjugaison. L'orbite de P pour cette action est réduite à $\{P\}$, puisque pour tout $g \in N_G(P)$, on a $gPg^{-1} = P$ par définition du normalisateur de P. De plus $P \subseteq N_G(P)$, et la transitivité de l'action de P sur $\mathrm{Syl}_7 \setminus \{P\}$ nous donne que $\mathrm{Syl}_7 \setminus \{P\}$ est une orbite à part entière de l'action de $N_G(P)$ sur Syl_7. On a donc :

$$\left|\mathrm{Stab}_{N_G(P)}(Q)\right| = \frac{|N_G(P)|}{|\mathcal{O}_Q|} = \frac{|N_G(P)|}{\left|\mathrm{Syl}_7 \setminus \{P\}\right|} = \frac{21}{8-1} = 3$$

On remarque que $\mathrm{Stab}_{N_G(P)}(Q)$ est l'ensemble des éléments de $N_G(P)$ qui laissent Q invariant par conjugaison, c'est donc $N_G(P) \cap N_G(Q) = M$, qui est donc un ensemble de cardinal 3.

On veut maintenant compter les sous-groupes d'ordre 3 de $N_G(P) \cup N_G(Q)$: il y en a 7 dans $N_G(P)$, 7 dans $N_G(Q)$, dont 1 qui est à la fois dans $N_G(P)$ et $N_G(Q)$, puisque M est d'ordre 3. Ainsi, $N_G(P) \cup N_G(Q)$ contient $7 + 7 - 1 = 13$ sous-groupes d'ordre 3.

Ce résultat nous donne qu'il y a plus de 13 sous-groupes d'ordre 3 dans G, or ces sous-groupes sont exactement les 3-Sylow. On a donc :

Propriétés.

- *Le groupe G admet exactement* 28 3*-Sylow.*

Nous avons, par les identités (♣) de la *page 28*, que $n_3 \in \{4, 7, 28\}$, et $n_3 \geqslant 13$. Une seule possibilité : $n_3 = 28$.

- *Le groupe G admet 56 éléments d'ordre 3.*

  En effet, les éléments d'ordre 3 sont tous contenus dans un des 3-Sylow. Or un 3-Sylow contient l'identité et $3-1 = 2$ éléments d'ordre 3, et il y a 28 3-Sylow, ce qui nous donne $2 \cdot 28 = 56$ éléments d'ordre 3 au total.

2.2.3 Les 2-Sylow de G

Dans la partie précédente, nous avions considéré P, Q deux 7-Sylow de G distincts, et nous avions posé $M = N_G(P) \cap N_G(Q)$. Nous avions vu que M était d'ordre 3 qui est donc un 3-Sylow de G.

On considère $N_G(M)$. C'est le normalisateur d'un groupe d'ordre 3 donc d'un 3-Sylow. Le théorème de Sylow nous donne alors que :

$$\left|N_G(M)\right| = \frac{|G|}{\left[G : N_G(M)\right]} = \frac{168}{n_3} = \frac{168}{28} = 6 \tag{♭}$$

Montrons par l'absurde que $N_G(M)$ n'est pas cyclique.

Supposons que $N_G(M)$ est cyclique. Puisque les 3-Sylow sont conjugués entre eux, les normalisateurs des 3-Sylow de G sont également conjugués.

En effet, si $S, T \in \mathrm{Syl}_3$, il existe $h \in G$ tel que $S = hTh^{-1}$, et alors :

$$\begin{aligned} N_G(S) &= \left\{g \in G \mid gSg^{-1} = S\right\} \\ &= \left\{g \in G \mid (gh)T(gh)^{-1} = hTh^{-1}\right\} \\ &= \left\{g \in G \mid (h^{-1}gh)T(h^{-1}gh)^{-1} = T\right\} \\ &= h\left\{g \in G \mid gTg^{-1} = T\right\}h^{-1} \\ &= hN_G(T)h^{-1} \end{aligned}$$

Il en résulte que tous les normalisateurs des 3-Sylow sont cycliques, et d'ordre 6.

Un groupe cyclique d'ordre 6 admet $\varphi(6) = (2-1)(3-1) = 2$ générateurs, c'est-à-dire que l'on trouve 2 éléments d'ordre 6 dans chaque normalisateur d'un 3-Sylow.

Pour se donner une idée du nombre d'éléments d'ordre 6 dans les normalisateurs des 3-Sylow, on commence par dénombrer les éléments d'ordre 6 communs à deux normalisateurs.

Soient $T_1, T_2 \in \mathrm{Syl}_3$ deux 3-Sylow distincts. Nous allons montrer que $N_G(T_1) \cap N_G(T_2)$ n'admet aucun élément d'ordre 6, et pour cela, nous avons besoin d'un résultat classique de théorie des groupes finis :

Lemme 2.2.3. *Soit G un groupe fini d'ordre pair. Alors G admet au plus $|G| - 2$ éléments $g \in G$ d'ordre $\mathrm{o}(g) \geqslant 3$.*

Démonstration. Soit G un groupe fini d'ordre pair, disons $|G| = 2n$. Par le théorème de Cauchy, G admet un élément d'ordre 2, ce qui nous donne que les éléments qui sont leur propre inverse est de cardinal $m \geqslant 2$. Ces éléments étant d'ordre 1 ou 2, nous avons que le nombre d'éléments d'ordre plus de 3 est de cardinal $2n - m \leqslant |G| - 2$. □

Il est alors impossible que $N_G(T_1) \cap N_G(T_2)$ admette un élément d'ordre 6, sinon $N_G(T_1)$ serait un groupe d'ordre 6 admettant au moins deux sous-groupes d'ordre 3, à savoir T_1 et T_2, supposés distincts. Il y aurait donc au moins $2(3-1) = 4$ éléments d'ordre 3, un élément d'ordre 6, donc au moins $4 + 1 = 5$ éléments d'ordre supérieur à 3. Or par le lemme précédent, $N_G(T_1)$ admet au plus $6 - 2 = 4$ éléments d'ordre supérieur à 3... contradiction.

Revenons-en à la preuve de non-cyclicité de $N_G(M)$.

Le calcul précédent montre que chaque normalisateur d'un 3-Sylow contient 2 éléments d'ordre 6, et que ces éléments ne se trouvent dans aucun autre normalisateur d'un autre 3-Sylow.

Cela nous donne que G admet au moins $2n_3 = 56$ éléments d'ordre 6 issus des normalisateurs des 3-Sylow. Ainsi G admet 1 éléments d'ordre 1, 56 éléments d'ordre 3 et autant d'ordre 6, ainsi que 48 éléments d'ordre 7. Mais G doit aussi admet également des 2-Sylow dont les éléments ne peuvent être d'ordre 3, 6 ou 7. Les 2-Sylow de G contiennent donc collectivement au plus $168 - (1 + 56 + 56 + 48) = 168 - 161 = 7$ éléments non-triviaux.

Un 2-Sylow de G est d'ordre $2^3 = 8$ et admet donc 7 éléments non-triviaux, il ne peut donc y avoir au plus qu'un seul 2-Sylow dans G, ce qui contredit sa simplicité... contradiction.

L'hypothèse de cyclicité de $N_G(M)$ conduit à une contradiction, d'où :

Propriété. *Le sous-groupe $N_G(M)$ n'est pas cyclique.*

On en déduit les propriétés suivantes :

Propriétés.

- *Le groupe G n'admet pas d'éléments d'ordre 6.*

  En effet, si $g \in G$ est d'ordre 6, alors $\left\langle g^2 \right\rangle$ est un sous-groupe d'ordre 3, donc un 3-Sylow de G, et $g \in N_G\left(\left\langle g^2 \right\rangle\right)$ qui contient alors g d'ordre 6, contredisant la non-cyclicité des normalisateurs des 3-Sylow.
- *Le groupe G n'admet pas d'éléments d'ordre 12, et en conséquence l'ordre d'un élément de G ne peut en réalité dépasser 8.*

  Si $g \in G$ est d'ordre 12, alors g^2 est d'ordre 6 dans G, ce qui contredit le premier point. En reprenant le tableau de la *page 29*, on voit que l'ordre le plus grand possible après 12 est l'ordre 8.

On remarque que $168 \mid 7! = 5040$, mais $168 \nmid 6! = 720$, et pour tout $n \leqslant 6$, $168 \nmid n!$ car $n!$ n'admet pas de facteur 7 dans sa décomposition en produit de facteurs premiers.
On en déduit :

Propriété. *Soit H un sous-groupe de G. Alors H est d'indice au moins 7 dans G.*

C'est une conséquence du *corollaire 2.1.6* et du petit calcul de la page précédente.

Nous avions déjà vu que $n_2 \in \{3, 7, 21\}$ à la liste des possibilités pour $(n_p)_{p\in\{2,3,7\}}$ (♣) de la *page 28*, et grâce à la propriété précédente, nous pouvons éliminer un cas : il ne peut en effet pas y avoir 3 2-Sylow, sinon, par le troisième point du théorème de Sylow, nous aurions que, pour tout $T \in \mathrm{Syl}_2$, $[G : N_G(T)] = 3$, ce qui contredit le fait que G ne peut admettre de sous-groupe d'indice plus petit que 7.
Ainsi $n_2 \in \{\cancel{3}, 7, 21\}$.

Notation. *Si $m \in \mathbb{N}^*$, nous noterons $\mathbf{O}_m$ l'ensemble des éléments de G d'ordre m.*

En reprenant la liste des différentes possibilités pour les nombres de p-Sylow (♣) de la *page 28*, il vient donc que :

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

Réécrivons cette égalité en terme de cardinal. Il vient :

$$168 = 1 + \left|\mathbf{O}_2\right| + 56 + \left|\mathbf{O}_4\right| + 48 + \left|\mathbf{O}_8\right| \quad \text{donc} \quad \left|\mathbf{O}_2\right| + \left|\mathbf{O}_4\right| + \left|\mathbf{O}_8\right| = 63$$

On remarque de plus que tout élément d'ordre que les éléments d'ordre 2, 4 et 8 sont des éléments d'ordre 2^α avec $\alpha \leqslant 3$, ces éléments engendrent ainsi des p-sous-groupes de G, et par le théorème de Sylow ces sous-groupes sont inclus dans les 2-Sylow de G, il vient donc, après avoir pris soin de retirer l'élément neutre de G :

$$\mathbf{O}_2 \sqcup \mathbf{O}_4 \sqcup \mathbf{O}_8 = \bigcup_{P\in\mathrm{Syl}_2} \left(P \setminus \left\{1_G\right\}\right)$$

Supposons que $n_2 = 7$. Alors on a, en reprenant l'égalité ensembliste précédente en terme de cardinal :

$$63 = \left|\bigcup_{P\in\mathrm{Syl}_2} \left(P \setminus \left\{1_G\right\}\right)\right| \leqslant \sum_{P\in\mathrm{Syl}_2} \left(2^3 - 1\right) = 7 \cdot 7 = 49$$

Il serait dommage d'avoir $63 \leqslant 49$, on ne peut donc pas avoir $n_2 = 7$, d'où :

Propriété. *Le groupe G possède exactement* 21 2*-Sylow.*

On ne peut pas avoir $n_2 = 7$ par le calcul précédent, et nous avions déjà éliminé $n_2 = 3$ en début de partie. On a donc que $n_2 \in \{\cancel{3}, \cancel{7}, 21\}$, il ne reste plus que $n_2 = 21$.

2.3 Une première preuve par les homographies

La stratégie que nous adoptons pour montrer l'unicité d'un groupe simple d'ordre 168 est d'identifier G avec un groupe connu. Pour cela, nous essaierons de fabriquer des homographies à l'aide d'éléments de G bien spécifiques.

2.3.1 Un système de générateurs pour G

On propose ici de montrer que G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$ grâce aux homographies. [4]

Comme dans la partie précédente, on prend $P, Q \in \mathrm{Syl}_7$ deux p-Sylow de G, avec $P \neq Q$. Ce sont deux sous-groupes d'ordre 7, donc cycliques et isomorphes à $\mathbb{Z}/7\mathbb{Z}$, et on peut donc choisir $\pi \in G$ un générateur de P.

Considérons l'application

$$\theta : \left\{ \begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathrm{Syl}_7 \setminus \{P\} \\ k & \longmapsto & \sigma_\pi^k(Q) \end{array} \right.$$

où σ_π est définie à la *page 29*, à l'égalité (★), c'est-à-dire que $\sigma_\pi^k(Q) = \pi^k Q \pi^{-k}$.

D'après le *lemme 2.2.2*, P agit sur $\mathrm{Syl}_p \setminus \{P\}$ par conjugaison, ce qui nous donne bien que $\sigma_\pi^k \in \mathrm{Syl}_7 \setminus \{P\}$ pour tout k dans $\mathbb{Z}/7\mathbb{Z}$, et cette action est transitive, ce qui nous donne de surcroît que l'application θ est surjective.

Puisque $\mathrm{Syl}_7 \setminus \{P\}$ comporte $8 - 1 = 7$ éléments, tout comme $\mathbb{Z}/7\mathbb{Z}$, θ est donc bijective.

On prolonge alors θ en $\theta(\infty) = P$ de sorte que θ soit une bijection $\theta : \widehat{\mathbb{F}_7} = \mathbb{P}^1\left(\mathbb{F}_7\right) \xrightarrow{\simeq} \mathrm{Syl}_7$.

On regarde de plus près l'application σ_π. C'est une application de Syl_7 dans lui-même, que l'on identifie à $\widehat{\mathbb{F}_7}$ grâce à l'application précédente. Ainsi, si $T \in \mathrm{Syl} \setminus \{P\}$, alors il existe $k \in \widehat{\mathbb{F}_7} \setminus \{\infty\} \simeq \mathbb{Z}/7\mathbb{Z}$ tel que $T = \sigma_\pi^k(Q) = \theta(k)$. Il vient alors que :

$$\sigma_\pi(T) = \sigma_\pi\left(\sigma_\pi^k(Q)\right) = \left(\pi\pi^k\right) Q \left(\pi^{-k}\pi^{-1}\right) = \pi^{k+1} Q \pi^{-(k+1)} = \theta(k+1)$$

Remarquons que l'on peut écrire $P = \theta(\infty)$ et que P est un point fixe de σ_π. Cela nous donne que σ_π peut se voir comme le 7-cycle $\left(0 \cdots 6\right)$, et à fortiori comme l'application $x \longmapsto x + 1$ grâce à θ.

Ainsi, σ_π est l'homographie $x \longmapsto \dfrac{1 \cdot x + 1}{0 \cdot x + 1}$ représentée par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Comme à la partie précédente, on pose $M = N_G(P) \cap N_G(Q)$. Rappelons-nous que M est un 3-Sylow de G d'ordre 3, il est donc cyclique et admet $\varphi(3) = 2$ générateurs.

Pour la suite, on prend α un des deux générateurs de M.

Nous avons que M et P sont des sous-groupes de $N_G(P)$, donc $\alpha \in M$ normalise P, d'où $\alpha\pi\alpha^{-1} \in P$, mais π est choisi générateur de P donc il existe $k \in \mathbb{Z}/7\mathbb{Z}$ tel que $\alpha\pi\alpha^{-1} = \pi^k$.

Que peut-on dire de la valeur de k ?

Propriété. *Vu comme un élément de $\mathbb{Z}/7\mathbb{Z}$, on a $k \in \{2, -3\}$.*

En effet, on montre par une courte récurrence que pour tout $n \in \mathbb{N}$, $\alpha^n \pi \alpha^{-n} = \pi^{k^n}$: cette égalité est immédiate pour $n = 0$ et si elle est vraie pour un certain $n \in \mathbb{N}$, alors :

$$\begin{aligned} \alpha^{n+1}\pi\alpha^{-n-1} &= \alpha^1 \pi^{k^n} \alpha^{-1} \\ &= \left(\alpha\pi\alpha^{-1}\right)^{k^n} \\ &= \left(\pi^k\right)^{k^n} = \pi^{k^{n+1}} \end{aligned}$$

Par principe de récurrence, on a alors que pour tout $n \in \mathbb{N}$, $\alpha^n \pi \alpha^{-n} = \pi^{k^n}$.

Puisque α est d'ordre 3, cette relation donne en particulier pour $n = 3$ que $\pi = \pi^{k^3}$, mais puisque π est d'ordre 7, on a $k^3 \equiv 1[7]$. Cela nous donne que $k \in \{1, 2, -3\}$.

En se souvenant que nous avions montré que $N_G(P)$ est non cyclique à la partie précédente, on s'aperçoit alors que $k \not\equiv 1[7]$ sinon on aurait que $\alpha\pi = \pi\alpha$ avec α et π deux éléments d'ordre premiers entre eux, ce qui implique que $o(\alpha\pi) = 21$, ce qui est impossible car $\alpha\pi$ serait alors un générateur de $N_G(P)$.

Ainsi $k \in \{2, -3\}$.

Cela nous permet d'en déduire le fait suivant :

Lemme 2.3.1. *Il existe $\mu \in N_G(P)$ tel que $\mu\pi\mu^{-1} = \pi^2$.*

Démonstration. En reprenant l'étude précédente, nous avions obtenu qu'il existait $k \in \{2, -3\}$ tel que $\alpha\pi\alpha^{-1} = \pi^k$.

- Si $k = 2$, on prend $\mu = \alpha$, ce qui nous donne bien $\mu\pi\mu^{-1} = \alpha\pi\alpha^{-1} = \pi^2$.
- Si $k = -3$, on prend $\mu = \alpha^2 = \alpha^{-1}$, ce qui nous donne $\mu\pi\mu = \alpha^2\pi\alpha = \pi^{(-3)^2} = \pi^9 = \pi^2$.

Dans les deux cas, on a trouvé $\mu \in N_G(P)$ tel que $\mu\pi\mu^{-1} = \pi^2$. □

On fixe donc une fois pour toute $\mu \in N_G(P)$ tel que $\mu\pi\mu^{-1} = \pi^2$.
Soit $k \in \mathbb{Z}$. Alors on a :

$$\left(\sigma_\mu\sigma_\pi^k\right)(Q) = \mu\pi^k Q\pi^{-k}\mu^{-1} = \mu\pi^k\mu^{-1}\mu Q\mu^{-1}\mu\pi^{-k}\mu^{-1}$$

Or $\mu \in M$ qui contient le normalisateur de Q, donc $\mu Q\mu^{-1} = Q$, d'où :

$$\left(\sigma_\mu\sigma_\pi^k\right)(Q) = \mu\pi^k\mu^{-1}Q\mu\pi^{-k}\mu^{-1} = \left(\mu\pi\mu^{-1}\right)^k Q\left(\mu\pi\mu^{-1}\right)^{-k} = \pi^{2k}Q\pi^{-2k} = \sigma_\pi^{2k}(Q)$$

Ainsi, si $T \in \mathrm{Syl}_7 \setminus \{P\}$, alors il existe $k \in \widehat{\mathbb{F}_7} \setminus \{\infty\}$ tel que $T = \sigma_\pi^k(Q) = \theta(k)$, et alors :

$$\sigma_\mu(T) = \theta(2k)$$

De plus, $\sigma_\mu(P) = \mu P\mu^{-1} = P$ car μ normalise P, et grâce à l'identification $\mathrm{Syl}_7 \simeq \widehat{F_7}$, on peut représenter σ_μ comme le produit de cycles $(1\,2\,4)\,(3\,6\,5)$, ou encore comme l'homographie $x \longmapsto \dfrac{2\cdot x + 0}{0\cdot x + 1}$ représentée par la matrice $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

Prenons cette fois-ci $\tau \in N_G(M) \setminus M$.
Nous avions montré à la partie précédente que $N_G(M)$ était un groupe d'ordre 6, or il n'y a que deux groupes d'ordre 6 à isomorphisme près : $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$. Nous avions également montré que $N_G(M)$ ne pouvait être cyclique, ainsi $N_G(M)$ est isomorphe à $\mathfrak{S}_3$, et en particulier, M contient donc un élément d'ordre 1, trois éléments d'ordre 2 et deux éléments d'ordre 3, ce qui correspond respectivement à l'identité, aux transpositions et aux 3-cycles de $\mathfrak{S}_3$.
Il est clair que $N_G(M)$ contient M qui contient 1 élément d'ordre 1 et deux éléments d'ordre 3, ainsi la seule possibilité pour $o(\tau)$ est 2.

Reprenons le même $\mu \in N_G(P)$ tel que dans le lemme précédent. Nous avons que $\mu \in M \subseteq N_G(M)$. Il vient alors que $\tau\mu\tau^{-1}$ est un élément de $N_G(M)$ d'ordre 3.
Or $N_G(M)$ n'admet que deux éléments d'ordre 3 qui sont μ et μ^{-1}. On remarque que $\tau\mu\tau^{-1}$ ne peut être égal à μ sinon on aurait que μ et τ commutent, et puisque leurs ordres sont premiers entre eux, $\tau\mu$ serait alors un élément d'ordre 6 dans $N_G(M)$, ce qui rendrait impossible que $N_G(M)$ soit isomorphe à $\mathfrak{S}_3$.
Ainsi $\tau\mu\tau^{-1} = \mu^{-1}$.

En utilisant le morphisme (★) de la *page 29* que l'on applique à l'égalité précédente, on obtient que :

$$\sigma_\tau\sigma_\mu\sigma_\tau^{-1} = \sigma_\mu^{-1}$$

Cette relation devient, grâce à l'identification $\mathrm{Syl}_7 \simeq \widehat{\mathbb{F}_7}$ et à l'écriture en cycles à supports disjoints de σ_μ :

$$\left(\sigma_\tau(1)\ \sigma_\tau(2)\ \sigma_\tau(4)\right)\left(\sigma_\tau(3)\ \sigma_\tau(6)\ \sigma_\tau(5)\right) = (1\ 4\ 2)\,(3\ 5\ 6)$$

On note que σ_τ ne peut admettre de points fixes : si $T \in \mathrm{Syl}_7$ vérifie $\sigma_\tau(T) = T$, cela signifie que τ normalise T, donc que $\tau \in N_G(T)$ qui est d'ordre 21 par le *lemme 2.2.1*, or τ est d'ordre 2, donc τ ne peut appartenir à un sous-groupe d'ordre impair.

On en déduit que :

Propriété. $\sigma_\tau(0) = \infty$

En effet, l'unicité de la décomposition en cycles à supports disjoints impose que $\sigma_\tau(0)$ soit un élément du support de σ_μ^{-1}, donc que $\sigma_\tau(0) \in \{0, \infty\}$, mais 0 ne peut être un point fixe, ce qui impose $\sigma_\tau(0) = \infty$.

On remarque également que :

$$\big(\sigma_\tau(1)\ \sigma_\tau(2)\ \sigma_\tau(4)\big) \neq \big(1\ 4\ 2\big)$$

En effet, si tel était le cas, σ_τ n'admettant pas de point fixes, on aurait deux possibilités pour $\sigma_\tau(1)$:

- Soit $\sigma_\tau(1) = 4$. Mais alors $\sigma_\tau(2)$ est « l'élément suivant » dans le cycle $\big(1\ 4\ 2\big)$, c'est-à-dire que $\sigma_\tau(2) = 2$, ce qui est impossible.
- Soit $\sigma_\tau(1) = 2$. Mais alors pour les mêmes raisons, on a $\sigma_\tau(4) = 4$ ce qui contredit une fois de plus le fait que σ_τ n'admet pas de points fixes.

Ainsi, par unicité de la décomposition en produit de cycles à supports disjoints, $\big(\sigma_\tau(1)\ \sigma_\tau(2)\ \sigma_\tau(4)\big)$ est l'unique 3-cycle différent de $\big(1\ 2\ 4\big)$:

$$\big(\sigma_\tau(1)\ \sigma_\tau(2)\ \sigma_\tau(4)\big) = \big(3\ 5\ 6\big)$$

En n'oubliant pas que σ_τ est nécessairement un élément d'ordre 2 n'ayant pas de points fixes, il ne reste que trois possibilités pour la décomposition en cycles à supports disjoints de σ_τ, à savoir :

Propriété. *L'élément τ est tel que :*

$$\sigma_\tau = \begin{cases} \gamma_1 \overset{def}{=} \big(0\ \infty\big)\big(1\ 3\big)\big(2\ 5\big)\big(4\ 6\big) & \\ \gamma_2 \overset{def}{=} \big(0\ \infty\big)\big(1\ 5\big)\big(2\ 6\big)\big(4\ 3\big) & \textit{ou} \\ \gamma_3 \overset{def}{=} \big(0\ \infty\big)\big(1\ 6\big)\big(2\ 3\big)\big(4\ 5\big) & \textit{ou} \end{cases}$$

Remarque. *Ces trois choix pour τ correspondent aux trois éléments de $N_G(M) \setminus M$ parmi lesquels nous avions pris τ.*

On choisit τ tel que $\sigma_\tau = \gamma_3 = \big(0\ \infty\big)\big(1\ 6\big)\big(2\ 3\big)\big(4\ 5\big)$. On calcule alors :

$$\begin{aligned} \sigma_\mu\sigma_\tau\sigma_\mu^{-1} &= \big(1\ 2\ 4\big)\big(3\ 6\ 5\big)\ \ \big(0\ \infty\big)\big(1\ 6\big)\big(2\ 3\big)\big(4\ 5\big)\ \ \big(1\ 4\ 2\big)\big(3\ 5\ 6\big) \\ &= \big(0\ \infty\big)\big(1\ 3\big)\big(2\ 5\big)\big(4\ 6\big) = \gamma_1 \end{aligned}$$

De même :

$$\begin{aligned} \sigma_\mu^2\sigma_\tau\sigma_\mu^{-2} &= \big(1\ 4\ 2\big)\big(3\ 5\ 6\big)\ \ \big(0\ \infty\big)\big(1\ 6\big)\big(2\ 3\big)\big(4\ 5\big)\ \ \big(1\ 2\ 4\big)\big(3\ 6\ 5\big) \\ &= \big(0\ \infty\big)\big(1\ 5\big)\big(2\ 6\big)\big(4\ 3\big) = \gamma_2 \end{aligned}$$

Ainsi on peut dans tous les cas obtenir les autres éléments de $N_G(M) \setminus M$ à l'aide de τ et de μ.

En remarquant que les paires $\{i, j\}$ avec $i, j \in \widehat{\mathbb{F}_7}$ tels que $\big(i\ j\big)$ apparaît dans la décomposition de σ_τ vérifient également que $j = -\dfrac{1}{i}$, on a que σ_τ peut-être représenté par l'homographie $x \longmapsto \dfrac{0 \cdot x - 1}{1 \cdot x + 0}$ qui a pour matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

On veut maintenant montrer que G est engendré par les éléments π, τ et γ. Pour cela nous utiliserons abondamment la partie 2.1.3.

Lemme 2.3.2. *Si G est un groupe simple d'ordre 168, alors G agit doublement transitivement sur* Syl_7.

Démonstration. Nous voulons appliquer la *proposition 2.1.8* à G : nous savons que G agit transitivement sur Syl_7 par conjugaison par le théorème de Sylow, et si nous fixons $P \in \mathrm{Syl}_7$, alors nous avons par le *lemme 2.2.2* que l'action de P

sur $\mathrm{Syl}_7 \setminus \{P\}$ était transitive, il en est donc de même pour $N_G(P)$.
On remarque que $N_G(P)$ est le stabilisateur de P sous l'action de G par conjugaison, ainsi par la *proposition 2.1.8*, G agit bien doublement transitivement sur Syl_7. □

On remarque alors que $N_G(P)$ est engendré par π et μ : π est d'ordre 7 donc engendre l'unique 7-Sylow de $N_G(P)$ qui est donc distingué dans $N_G(P)$, et μ est d'ordre 3. Ainsi $\langle\pi\rangle \cap \langle\mu\rangle = \{1\}$ et $|N_G(P)| = |\langle\pi\rangle| \cdot |\langle\mu\rangle| = 21$, cela nous donne que $N_G(P) = \langle\pi\rangle \rtimes_\varphi \langle\mu\rangle$ qui est engendré par π et μ.

Donc $\langle\pi, \mu, \tau\rangle$ est un sous-groupe de G contenant $\langle\pi, \mu\rangle = N_G(P)$ et $\tau \in G \setminus N_G(P)$, par le *corollaire 2.1.10*, nous avons :

Propriété. $G = \langle\pi, \mu, \tau\rangle$

2.3.2 Conditions d'appartenance à $\mathrm{PSL}_2(k)$

On se pose ici le problème suivant :
Étant donné $u \in \mathrm{GL}_2(k)$, à quelle(s) condition(s) la projection $\overline{u}$ de u dans $\mathrm{PGL}_2(k) \overset{\text{def}}{=} \mathrm{GL}_2(k)/Z\left(\mathrm{GL}_2(k)\right)$ est dans $\mathrm{PSL}_2(k)$?

Puisque $\mathrm{SL}_2(k)$ est un sous-groupe de $\mathrm{GL}_2(k)$, nous avons que son image par la projection dans $\mathrm{PGL}_2(k)$, à savoir $\mathrm{PSL}_2(k)$ s'injecte dans $\mathrm{PGL}_2(k)$, c'est-à-dire que l'on a, en notant $\pi : \mathrm{GL}_2(k) \longmapsto \mathrm{PGL}_2(k)$ l'application de passage au quotient :

$$\begin{array}{ccc} \mathrm{SL}_2(k) & \hookrightarrow & \mathrm{GL}_2(k) \\ \downarrow{\scriptstyle \pi|_{\mathrm{SL}_2(k)}} & & \downarrow{\scriptstyle \pi} \\ \mathrm{PSL}_2(k) & \hookrightarrow & \mathrm{PGL}_2(k) \end{array}$$

- Si $\overline{u} \in \mathrm{PSL}_2(k)$, alors on sait qu'il existe $v \in \mathrm{SL}_2(k)$ tel que $\pi(v) = \overline{u}$ ce qui se traduit par l'existence d'un certain $\lambda \in k^\times$ tel que $u = \lambda v$, et donc $\det(u) = \lambda^2 \det(v) = \lambda^2$.
  Mais on sait que $\det(u) \in k^\times$, on a donc que $\det(u)$ est un carré dans $k^\times$.
  On peut donc conjecturer que le fait d'avoir $\det(u)$ un carré dans $k^\times$ est une condition nécessaire et suffisante pour que $\overline{u} \in \mathrm{PSL}_2(k)$.
- Réciproquement, si $\det(u)$ est un carré dans $k^\times$, on veut montrer que $\overline{u} \in \mathrm{PSL}_2(k)$.
  On sait alors qu'il existe $\lambda \in k^\times$ tel que $\det(u) = k^2$.
  On constate que l'endomorphisme $v \overset{\text{def}}{=} \lambda^{-1}u$ a alors un déterminant de 1, donc $v \in \mathrm{SL}_2(k)$, et $\overline{v} = \pi(v) = \pi\left(\lambda^{-1}u\right) = \overline{u} \in \mathrm{SL}_2(k)$

D'où :

Proposition 2.3.3. *Un élément de $\overline{u} \in \mathrm{PGL}_2(k)$ est dans $\mathrm{PSL}_2(k)$ si et seulement si $\overline{u}$ est une homographie de déterminant un carré dans $k^\times$.*

En particulier, les homographies σ_π, σ_μ et σ_τ déterminées à la partie précédente, et qui sont représentées par les trois matrices :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Ces trois matrices ont pour déterminant 1, 2 et 1, or dans $\mathbb{F}_7$, nous avons que $1^2 = 1$ et $4^2 = 16 = 2$, donc les homographies σ_π, σ_μ et σ_τ sont dans $\mathrm{PSL}_2(\mathbb{F}_7)$.

Remarque. *Nous avons donc obtenu un renforcement de ce que nous avions déterminé à la* partie 1.3.3 *puisque nous venons d'expliquer que les homographies r, t et δ de la* partie 1.3.3 *sont en réalité des éléments de $\mathrm{PSL}_2(\mathbb{F}_7)$, ce qui donne que $\mathrm{PSL}_2(\mathbb{F}_7) = \langle r, t, \delta\rangle$.*

2.3.3 L'unicité du groupe simple d'ordre 168

Les deux parties précédentes vont nous permettre de voir que G est nécessairement isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$.

On considère le morphisme induit par l'action par conjugaison de G sur Syl_7, qui envoie un élément $g \in G$ sur σ_g défini par :

$$\forall g \in G, \quad \varphi(g) \overset{\text{def}}{=} \sigma_g : \left\{ \begin{array}{ccc} \mathrm{Syl}_7 & \longrightarrow & \mathrm{Syl}_7 \\ T & \longmapsto & gTg^{-1} \end{array} \right.$$

Nous l'avions déjà introduit à la *page 29*, à l'égalité (★).

On remarque que les éléments π, μ et τ sont envoyés par φ sur les homographies représentées par les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Ces matrices sont de déterminant un carré dans $\mathbb{F}_7^\times$, donc appartiennent bien à $\mathrm{PSL}_2(\mathbb{F}_7)$, et nous avions vu à la *partie 1.3.3* qu'elles engendrent $\mathrm{PSL}_2(\mathbb{F}_7)$. Ainsi le morphisme φ se restreint à un isomorphisme $G \longrightarrow H \leqslant \mathfrak{S}\left(\mathrm{Syl}_7\right)$ vers H un sous-groupe de $\mathfrak{S}\left(\mathrm{Syl}_7\right)$ isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$, d'où :

Propriété. *Le groupe G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$.*

On en déduit le principal théorème de cette partie :

Théorème 2.3.4 (Unicité du groupe simple d'ordre 168)**.** *Il existe un unique groupe simple d'ordre* 168.

Démonstration. Toute la *partie 2.3* nous a permis de montrer que si G est un groupe simple d'ordre 168, alors G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$, ce qui nous donne l'unicité ; et la *partie 1* nous donne que $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2)$ est un groupe simple d'ordre 168, ce qui nous donne l'existence. □

2.4 Plan de Fano

Nous reprenons G un groupe simple d'ordre 168.

Dans cette partie, nous nous évertuerons à montrer l'unicité d'un groupe simple d'ordre 168 d'une autre manière, en exploitant les propriétés géométriques que l'on peut conférer à certains sous-groupes de G isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2.4.1 Rappels sur $\mathfrak{S}_4$ et D_8

On rappelle ici quelques propriétés du groupe symétrique $\mathfrak{S}_4$ et du groupe diédral D_8.

Remarque. *J'utilise la notation D_{2n} pour le groupe diédral d'ordre $2n$, c'est-à-dire le groupe des isométries du plan laissant invariant un n-gone régulier.*
Le groupe D_8 désigne donc celui qui laisse invariant un carré.

Théorème 2.4.1 (Propriétés de $\mathfrak{S}_4$)**.** *On considère le groupe $\mathfrak{S}_4$. Alors :*

(1) *Il y a un unique sous-groupe distingué d'ordre* 4*, que l'on appelle groupe de Klein* K*, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(2) *Il y a trois autres sous-groupes d'ordre* 4 *et isomorphes à* K *dans $\mathfrak{S}_4$, et ces trois groupes sont conjugués entre eux, mais ne sont pas conjugués à* K*, car $\mathrm{K} \lhd \mathfrak{S}_4$.*

(3) *Si K_1, K_2 sont deux de ces trois groupes de Klein non distingués, alors $\langle K_1, K_2 \rangle = \mathfrak{S}_4$.*

(4) *Si K' est un sous-groupe de $\mathfrak{S}_4$ isomorphe à* K *mais non distingué, alors $K'\mathrm{K} \simeq \mathrm{K}K' \simeq \mathrm{D}_8$.*

(5) *Les* 2*-Sylow de $\mathfrak{S}_4$ sont isomorphes au groupe diédral D_8.*

Théorème 2.4.2 (Propriétés de D_8)**.** *Le groupe* D_8 *satisfait les propriétés suivantes :*

(1) *Le centre de* D_8 *est engendré par un élément d'ordre* 2*, disons* τ*.*

(2) *Il y a exactement trois sous-groupes d'ordre* 4 *dans* D_8*, tous distingués, dont un est cyclique et les autres sont isomorphes à* K*.*

(3) *Si* K' *est un des sous-groupe de* D_8 *isomorphe à* K*, alors un système de générateur de* K' *est donné par* $\{\tau, w\}$*, où* $\langle\tau\rangle = Z(\mathrm{D}_8)$*.*

2.4.2 Groupes de Klein de G

On se donne à nouveau G un groupe simple d'ordre 168.

Lemme 2.4.3. *Il existe une paire de* 2*-Sylow de* G *distincts ayant une intersection non-triviale.*

Démonstration. Supposons au contraire que pour tout $T_1, T_2 \in \mathrm{Syl}_2$ avec $T_1 \neq T_2$, $T_1 \cap T_2 = \{1_G\}$. Alors tous les $\left(T \setminus \{1_G\}\right)_{T\in\mathrm{Syl}_2}$ sont disjoints, et contiennent tous les éléments d'ordre 2, 4 ou 8. Nous savons qu'il y a 21 2-Sylow dans G, ainsi G contient $7 \cdot 21 = 147$ éléments d'ordre 2, 4 ou 8. Il y a aussi un élément d'ordre 1, 48 éléments d'ordre 7 et 56 éléments d'ordre 3. Ainsi $168 = |G| \geqslant 1 + 147 + 48 + 56 = 252$, absurde !
Il existe ainsi au moins une paire de 2-Sylow distincts d'intersection non-triviale. □

Lemme 2.4.4. *Si* G *a plus d'un* p*-Sylow pour un certain* p *premier et que* $P, Q \in \mathrm{Syl}_p$ *sont distincts et tels que* $|P \cap Q|$ *est maximal, alors :*

(i) Le groupe $N_G(P \cap Q)$ *admet plus d'un* p*-Sylow.*

(ii) Toute paire de p*-Sylow distincts de* $N_G(P \cap Q)$ *admettent* $P \cap Q$ *comme intersection.*

Démonstration. (i) Soient $P, Q \in \mathrm{Syl}_p$ distincts. Alors $P \cap Q \subsetneq P$, et donc $P \cap Q \subsetneq N_P(P \cap Q)$.
Soit maintenant T un p-Sylow de $N_G(P \cap Q)$ contenant $N_P(P \cap Q)$. C'est un p-sous-groupe de G, et il existe donc $U \in \mathrm{Syl}_p$ tel que $P \subseteq U$.
Supposons dans un premier temps que $P \neq U$. Alors $P \cap Q \subsetneq N_P(P \cap Q) \subseteq T \subseteq U$. Mais $N_P(P \cap Q) \subseteq P$, donc $P \cap Q \subsetneq N_P(P \cap Q) \subseteq P \cap U$, contredisant ainsi la maximalité de $|P \cap Q|$. Ainsi $U = P$.
Or $T \subseteq P$ et $T \subseteq N_G(P \cap Q)$ donc $T \subseteq P \cap N_G(P \cap Q) = N_P(P \cap Q)$; et par hypothèse $N_P(P \cap Q) \subseteq T$, d'où $T = N_P(P \cap Q)$.
En reproduisant le même raisonnement avec $S \in \mathrm{Syl}_p\left(N_G(P \cap Q)\right)$ contenant $N_Q(P \cap Q)$, on montre cette fois-ci que $S = N_Q(P \cap Q)$.
Les groupes T et S sont deux p-Sylow de $N_G(P \cap Q)$, et nous voulons désormais montrer qu'ils sont distincts.
Supposons que $T = S$. Alors $N_P(P \cap Q) \subseteq P$ par définition du normalisateur, et :

$$N_P(P \cap Q) = T = S = N_Q(P \cap Q) \subseteq Q$$

Ainsi $N_P(P \cap Q) \subseteq P \cap Q$, c'est-à-dire que l'on a :

$$P \cap Q \subsetneq N_P(P \cap Q) \subseteq P \cap Q$$

Ce qui est totalement contradictoire ! Ainsi T et S sont deux p-Sylow de $N_G(P \cap Q)$ distincts.

(ii) On a $P \cap Q \lhd N_G(P \cap Q)$, donc un p-Sylow de $N_G(P \cap Q)$ contient nécessairement $P \cap Q$. L'intersection de deux p-Sylow de $N_G(P \cap Q)$ contient donc $P \cap Q$.
Pour l'autre inclusion, rappelons-nous de la démonstration du point (i) : un p-Sylow de $N_G(P \cap Q)$ est de la forme $T \cap N_G(P \cap Q)$ pour un certain $T \in \mathrm{Syl}_p$. Ainsi l'intersection de deux p-Sylow de $N_G(P \cap Q)$ peut-être vue comme $T \cap S \cap N_G(P \cap Q)$ pour deux $T, S \in \mathrm{Syl}_p$. En notant n l'ordre de ce groupe, nous avons $|T \cap S| \leqslant n \leqslant |P \cap Q|$ par maximalité de $|P \cap Q|$. L'intersection de deux p-Sylow de $N_G(P \cap Q)$ contient donc $P \cap Q$ et à un ordre plus petit, ainsi $P \cap Q$ est nécessairement cette intersection.

□

Proposition 2.4.5. *Le normalisateur de la plus grande intersection de deux 2-Sylow distincts de G est isomorphe à $\mathfrak{S}_4$.*

Démonstration. Parmi toutes les paires de 2-Sylow possibles, prenons $(T_1, T_2) \in \mathrm{Syl}_2 \times \mathrm{Syl}_2$ tel que $U \overset{\text{def}}{=} T_1 \cap T_2$ soit d'ordre maximal, avec $T_1 \neq T_2$.
L'ordre d'un 2-Sylow de G étant 8 et puisqu'il existe au moins une paire de 2-Sylow d'intersection non-triviale, U est donc de cardinal 2 ou 4.
Par le lemme N/C (*lemme 2.1.11*), $N_G(U)/C_G(U)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(U)$. En remarquant que $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = \{1\}$, $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3$, on a que $\mathrm{Aut}(U)$ est à isomorphisme près un des groupes $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$ ou $\mathfrak{S}_3$. En particulier aucun de ses groupes n'a pour ordre un multiple de 7, donc 7 ne peut diviser $|N_G(U)/C_G(U)|$.
Cela nous donne que si $N_G(U)$ contient un sous-groupe d'ordre 7, alors ce groupe est aussi contenu dans $C_G(U)$ sans quoi $N_G(U)/C_G(U)$ aurait un ordre multiple de 7.
Supposons que $N_G(U)$ contienne un sous-groupe d'ordre 7. Par ce qui précède, ce sous-groupe commute avec tous les éléments de U, et en particulier ce sous-groupe est un 7-Sylow de G normalisé par un élément d'ordre 2. Appelons x cet élément d'ordre 2, nous avons que $x \in N_G(P)$. Or par le *lemme 2.2.1*, on sait que $N_G(P)$ est d'ordre 21, et donc $|\langle x \rangle| = 2 \mid 21$... absurde !
Ainsi $|N_G(U)|$ n'est pas divisible par 7, et donc :

$$|N_G(U)| \in \left\{2, 2^2, 2^3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3\right\}$$

Par le point (i) du *lemme 2.4.4* prédécent, $N_G(U)$ admet au moins deux 2-Sylow distincts, ainsi $N_G(U)$ ne peut-être un 2-groupe sans quoi $N_G(U)$ serait son propre unique 2-Sylow. De plus, l'intersection de deux 2-Sylow distincts de $N_G(U)$ est exactement $U = T_1 \cap T_2$ par le point (ii) du *lemme 2.4.4* qui est de cardinal au moins 2, ce qui nous donne que les 2-Sylow de $N_G(U)$ sont d'ordre au moins 2^2, et donc que $|N_G(U)|$ est un multiple de 2^2. Cela restreint donc les cardinaux possibles à :

$$|N_G(U)| \in \left\{2^2 \cdot 3, 2^3 \cdot 3\right\}$$

Soit P un 3-Sylow de $N_G(U)$. Alors $P \in \mathrm{Syl}_3$ et son normalisateur dans G $N_G(P)$ est d'ordre $\dfrac{|G|}{[G : N_G(P)]} = \dfrac{168}{28} = 6$.
Puisque $N_{N_G(U)}(P)$ est un sous-groupe de $N_G(P)$ contenant P, $\left|N_{N_G(U)}(P)\right| \in \{3, 6\}$. Sachant que $|N_G(U)| \in \{12, 24\}$, on a que les valeurs possibles pour $\left[N_G(U) : N_{N_G(U)}(P)\right]$ sont $\{2, 4, 8\}$. Or par le théorème de Sylow, cet indice est également le nombre de 3-Sylow de $N_G(U)$, qui ne peut valoir que 1 ou 4.
Ainsi $N_G(U)$ admet exactement 4 3-Sylow.

On a que $|N_G(U)| \in \{12, 24\}$.
Si $N_G(U)$ est d'ordre 12, alors $N_G(U)$ est isomorphe à un des cinq groupes suivants :

$$\mathbb{Z}/12\mathbb{Z} \qquad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z} \qquad \mathrm{D}_{12} \qquad \mathfrak{A}_4$$

où la loi de groupe de $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$ est donnée par :

$$(n, m) \cdot \left(n', m'\right) = \left(n + (-1)^m n', m + m'\right)$$

Le seul de ces cinq groupes a admettre exactement 4 3-Sylow est $\mathfrak{A}_4$. Mais $\mathfrak{A}_4$ a un unique 2-Sylow et $N_G(U)$ en a au moins deux. Il apparaît donc que $N_G(U)$ n'est isomorphe à aucun des cinq groupes précédents, ce qui est absurde.

Ainsi, $|N_G(U)| = 24$, et donc $\left|N_{N_G(U)}(P)\right| = 6$.
Faisons agir $N_G(U)$ par conjugaison sur ses 4 3-Sylow. Cette action induit un morphisme $\varrho : N_G(U) \longrightarrow \mathfrak{S}_4$. Le noyau $\ker \varrho$ de ce morphisme est alors exactement l'intersection des normalisateurs des 3-Sylow de $N_G(U)$, par définition de ses normalisateurs.
Supposons que $\ker \varrho \neq \{1\}$. Alors, puisque $\ker \varrho \subseteq N_{N_G(U)}(P)$, nous avons que $|\ker \varrho|$ divise 6. Puisque P ne normalise aucun autre 3-Sylow, P n'est pas un sous-groupe de $\ker \varrho$, mais $P \subseteq N_{N_G(U)}(P)$ et P est de cardinal 3, ce qui nous donne que $|\ker \varrho| \neq 3, 6$, autrement dit que $|\ker \varrho| = 2$.
On a alors que le groupe $N_G(U)/\ker \varrho$ est d'ordre 12 et possède plusieurs 2-Sylow distincts et 4 3-Sylow correspondant aux 2, 3-Sylow de $N_G(U)$ quotientés par $\ker \varrho$. Grâce à la généalogie des groupes d'ordre 12, on sait que le groupe $N_G(U)/\ker \varrho$ n'est alors isomorphe à aucun des cinq groupes d'ordre 12 à isomorphisme près, ce qui est absurde.

Ainsi $\ker \varrho = \{1\}$ et le morphisme ϱ est injectif. Par égalité des ordres de $N_G(U)$ et de $\mathfrak{S}_4$, nous avons donc le résultat voulu :

$$N_G(U) \simeq \mathfrak{S}_4$$

□

Corollaire 2.4.6. *Dans G, la plus grande intersection de deux 2-Sylow distincts est un groupe isomorphe au 4-groupe de Klein* K.

Démonstration. Prenons $T_1, T_2 \in \mathrm{Syl}_2$ d'intersection d'ordre maximal, et $U = T_1 \cap T_2$. Alors $U \lhd N_G(U) \simeq \mathfrak{S}_4$, donc U est à isomorphisme près un des groupes suivants :

$$\{1\} \qquad \mathrm{K} \qquad \mathfrak{A}_4 \qquad \mathfrak{S}_4$$

Or on sait que U est d'ordre 2 ou 4, il n'y a ainsi qu'une seule possibilité : $U \simeq \mathrm{K}$. □

Corollaire 2.4.7. *Les 2-Sylow de G sont isomorphes au groupe diédral* D_8.

Démonstration. Soient $T_1, T_2 \in \mathrm{Syl}_2$ deux 2-Sylow distincts d'intersection maximale, et posons à nouveau $U = T_1 \cap T_2$. Nous avons alors que $N_G(U) \simeq \mathfrak{S}_4$ et qu'un 2-Sylow de $N_G(U)$ est un 2-Sylow de G. Ce 2-Sylow est donc isomorphe à un 2-Sylow de $\mathfrak{S}_4$. Or les 2-Sylow de $\mathfrak{S}_4$ sont isomorphes à D_8.
De plus, tous les 2-Sylow de G sont conjugués et donc isomorphes entre eux, ainsi tout 2-Sylow de G est isomorphe à D_8. □

Lemme 2.4.8. *Soit G un groupe fini et p premier divisant $|G|$. Soit P un p-Sylow et soient U, W deux sous-groupes distingués dans P. Alors U et W sont conjugués dans G si et seulement si ils le sont aussi dans $N_G(P)$.*

Démonstration. Soient $P \in \mathrm{Syl}_p$ et $U, W \lhd P$.

- ($\Longleftarrow$) Il n'y a rien à faire : si U et W sont conjugués dans $N_G(P)$, ils le sont évidement dans G puisque $N_G(P) \subseteq G$.
- ($\Longrightarrow$) Supposons que U et W sont conjugués dans G : il existe donc $g \in G$ tel que $gUg^{-1} = W$. Puisque $U \lhd P$, on a que $W \lhd gPg^{-1}$, mais aussi $W \lhd P$, donc $W \lhd H \overset{\text{def}}{=} \left\langle P, gPg^{-1} \right\rangle$. Les sous-groupes P et gPg^{-1} sont des p-Sylow de H, ils sont donc conjugués dans H : il existe $h \in H$ tel que $hgPg^{-1}h^{-1} = P$. Ainsi $gh \in N_G(P)$, et $hgU(hg)^{-1} = hWh^{-1}$. Puisque $W \lhd P \lhd H$, $hWh^{-1} = W$ et donc $hgU(hg)^{-1} = W$: U et W sont conjugués dans $N_G(P)$.

□

Lemme 2.4.9. *Un 2-Sylow est son propre normalisateur dans G.*

Démonstration. Soit $T \in \mathrm{Syl}_2$.

- On sait que dans G aucun élément d'ordre 2 ne commute avec un élément d'ordre 7 : un tel élément d'ordre 2 serait dans le normalisateur d'un sous-groupes d'ordre 7, donc dans le normalisateur d'un 7-Sylow ; ces normalisateurs étant d'ordre 21, ils ne peuvent pas contenir d'éléments d'ordre 2.
  De même, un élément d'ordre 2 ne peut commuter avec un élément d'ordre 3, sinon leur produit serait d'ordre 6 et G ne contient aucun élément d'ordre 6 par une propriété de la *page 32*.

  Ainsi, il n'y a aucun élément d'ordre 2 qui commute avec un élément d'ordre impair.
  On sait que $T \simeq \mathrm{D}_8$, donc son centre est $Z(T) = \langle \tau \rangle$ pour τ un certain élément d'ordre 2. Regardons le centralisateur de cet élément d'ordre 2 : $C_G(\tau)$ ne contient aucun élément d'ordre pair, donc $|C_G(\tau)| \in \left\{2, 2^2, 2^3\right\}$. Mais puisque τ engendre le centre de τ, nous avons que tout élément de T commute avec τ, et donc $T \subseteq C_G(\tau)$, et puisque $|T| = 8$, nous avons $C_G(\tau) = T$.
- On constate maintenant que T se normalise lui-même, et tout élément qui normalise T normalise aussi son centre $Z(T)$, et donc un élément de $N_G(T)$ commute avec τ, où $\langle \tau \rangle = Z(T)$, donc $N_G(T) \leqslant C_G(\tau) = T$.
  Ainsi $T \subseteq N_G(T) \subseteq T$, d'où $T = N_G(T)$.

□

Proposition 2.4.10. *Les 2-Sylow de G contiennent deux sous-groupes distingués U et W tous deux isomorphes au groupe de Klein* K *mais non conjugués dans G.*

Démonstration. Soit P un 2-Sylow de G. Nous avons vu que P est isomorphe à D_8, et ce on sait que ce groupe admet exactement 3 sous-groupes d'ordre 4, donc d'indice 2, et donc distingués par le théorème de Frobenius. Un de ces sous-groupes est cyclique isomorphe à $\mathbb{Z}/4\mathbb{Z}$, et les deux autres sont non cycliques isomorphes à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \simeq$ K.

Appelons U et W ces deux sous-groupes, et montrons qu'ils ne sont pas conjugués dans G. Pour cela, nous allons utiliser le *lemme 2.4.8*, et plutôt montrer que U et W ne sont pas conjugués dans $N_G(P)$. Or par le *lemme 2.4.9*, $N_G(P) = P$.

Il nous faut donc montrer que U et W ne sont pas conjugués dans $P \simeq D_8$. Or U et W sont tous les deux distingués dans P car d'indice 2, donc pour tout élément $g \in P$, $gUg^{-1} = U \neq W$: U et W ne sont donc pas conjugués dans $N_G(P)$, donc ne sont pas conjugués dans G. □

2.4.3 Relation entre les groupes de Klein de G

Dans toute cette partie, nous fixons P un 2-Sylow de G, et nous posons U et W les deux sous-groupes de T isomorphes au groupe de Klein K, avec U et W non conjugués dans G, ce qu'il est possible de faire en vertu de la *proposition 2.4.10*.

Théorème 2.4.11. *Si G est un groupe et S une partie de G, alors le nombre de conjugués de S est l'indice $\left[G : N_G(S)\right]$. En particulier, le nombre de conjugués d'un élément s est alors $\left[G : C_G(s)\right]$.*

Lemme 2.4.12. *Un groupe simple à* 168 *éléments G n'admet qu'une seule classe d'éléments d'ordre* 2.

Démonstration. Dans la première partie nous avions montré que les ordre possibles pour les éléments d'ordre pair dans G étaient $2, 4$ ou 8 : ce ne sont que des puissances de 2, ainsi ces éléments sont contenus dans les 2-Sylow de G.
Or, on sait que chaque 2-Sylow est isomorphe à D_8 qui ne contient aucun élément d'ordre 8, ce qui permet déjà d'affirmer que G ne contient aucun élément d'ordre 8.
De plus, chaque 2-Sylow contient exactement deux éléments d'ordre 4, et puisqu'il y a 21 2-Sylow dans G, on en déduit qu'il y a *au plus* $2 \cdot 21 = 42$ éléments d'ordre 4 dans G. Pour affirmer qu'il y a exactement 42 éléments d'ordre 4 dans G, il nous faut montrer qu'il n'y a aucun élément d'ordre 4 dans une intersection de deux 2-Sylow distincts.
Or, si T_1 et T_2 sont deux 2-Sylow distincts et qu'on veut avoir une chance de trouver un élément d'ordre 4 dans leur intersection, il faut que $|T_1 \cap T_2| \geqslant 4$, c'est-à-dire que $|T_1 \cap T_2|$ soit maximal. En posant $U = T_1 \cap T_2$, on sait que U est l'unique 2-Sylow de $N_G(U)$ qui est isomorphe à $\mathfrak{S}_4$ par la *proposition 2.4.5*. Puisque $\mathfrak{S}_4$ admet K comme unique 2-Sylow, nous avons que $U \simeq$ K et donc ne contient aucun élément d'ordre 4.
Ainsi il y a exactement 42 éléments d'ordre 4 dans G.
Sachant qu'il y a 1 élément d'ordre 1, 56 éléments d'ordre 3, 42 éléments d'ordre 4 et 48 éléments d'ordre 7, on sait qu'il y a $168 - 1 - 56 - 42 - 48 = 21$ éléments d'ordre 2 dans G.

Maintenant, souvenons-nous de la preuve du *lemme 2.4.9* : nous avions vu qu'il était possible de prendre τ un élément de G d'ordre 2 tel que $C_G(\tau)$ soit un 2-Sylow. Par le théorème précédent, cet élément admet alors $\left[G : C_G(\tau)\right] = \dfrac{168}{8} = 21$ conjugués, soit autant de conjugués que d'éléments d'ordre 2, les éléments d'ordre 2 se trouvent donc dans une même et unique classe. □

Propriété. *Les groupes U et W ont des normalisateurs isomorphes à $\mathfrak{S}_4$ et admettent exactement* 7 *conjugués chacun.*

En effet, on peut écrire $W = \langle w, \tau\rangle$ pour un certain w et τ avec $\langle\tau\rangle = Z(T)$ et w et τ d'ordre 2, car $T \simeq D_8$ et $W \simeq$ K $\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Puisqu'il n'y a qu'une seule classe d'éléments d'ordre 2, les éléments w et τ sont conjugués et $C_G(w) \simeq C_G(\tau)$ et $W \subseteq C_G(w) \cap P$. Maintenant, $P \neq C_G(w)$, sinon élément de P commuterait avec w, et donc $w \in Z(P)$, ce qui donnerait que $w = \tau$ par égalité de leurs ordres, et $W = \langle\tau, w\rangle \simeq \mathbb{Z}/2\mathbb{Z} \not\simeq$ K. Ainsi $C_G(w) \cap P$ est l'intersection de deux 2-Sylow distincts, et cette intersection est de cardinal 4 donc maximal : par la *proposition 2.4.5*, $N_G(W) \simeq \mathfrak{S}_4$.

Le *théorème 2.4.11* nous indique alors que W a exactement $\left[G : N_G(W)\right] = \frac{168}{24} = 7$ conjugués.
Le même procédé appliqué à U montre que U a également 7 conjugués.

Notation. *Nous noterons U_i et W_i le i-ème conjugué de U et de W, avec $i \in [\![1,7]\!]$ et la convention $U = U_1$, $W = W_1$.*

Proposition 2.4.13. *Chaque W_i, $i \in [\![1,7]\!]$ est normalisé par exactement trois des $\left\{U_j\right\}_{j\in[\![1,7]\!]}$.*

Démonstration. Regardons $N_G\left(W_i\right)$. Nous savons qu'il est isomorphe à $\mathfrak{S}_4$ par la propriété précédente, et W_i est l'unique sous-groupe distingué isomorphe à K dans $\mathfrak{S}_4$.
On sait toutefois que $\mathfrak{S}_4$ admet trois autres sous-groupes isomorphes à K non distingués dans $\mathfrak{S}_4$, ainsi on peut trouver trois sous-groupes de $N_G\left(W_i\right)$, H_1, H_2, $H_3 \simeq$ K distincts de W_i, et donc H_1 ,H_2, H_3 font partie des $\left\{U_k, W_j\right\}_{j\neq i}$.
De plus, aucun des H_1, H_2 et H_3 n'est conjugué à W_i puisque $W_i \lhd N_G\left(W_i\right)$; on en déduit donc que H_1, H_2, H_3 font partie des $\{U_j\}_{j\in[\![1,7]\!]}$. □

Corollaire 2.4.14. *Chaque U_i, $i \in [\![1,7]\!]$ normalise exactement trois des $\left\{W_j\right\}_{j\in[\![1,7]\!]}$.*

Démonstration. Soit $i \in [\![1,7]\!]$. Supposons que U_i normalise W_j. Alors W_j est un sous-groupe de $N_G\left(U_i\right) \simeq \mathfrak{S}_4$. Dans $\mathfrak{S}_4$, le produit du groupe de Klein distingué par un des autres sous-groupe isomorphe au groupe de Klein est un groupe isomorphe à D_8, ainsi $U_iW_j \simeq D_8 \simeq W_jU_i$, et donc W_j normalise U_i. En remarquant que l'on peut appliquer la même preuve de la proposition précédente en inversant les $\{U_k\}_{k\in[\![1,7]\!]}$ et les $\{W_k\}_{k\in[\![1,7]\!]}$, on a que U_i est normalisé par exactement trois des $\{W_k\}_{k\in[\![1,7]\!]}$, qui sont alors eux-mêmes normalisés par U_i.
On remarque alors que si U_i normalise un autre W_k, alors U_i serait normalisé par quatre des $\{W_k\}_{k\in[\![1,7]\!]}$, contredisant la proposition précédente. □

Proposition 2.4.15. *Pour chaque $U_i \neq U_j$, il existe exactement un W_k qui soit normalisé à la fois par U_i et U_j.*

Démonstration. Soient $i, j \in [\![1,7]\!]$, $i \neq j$.

Dans un premier temps, montrons qu'il existe *au plus* un tel W_k.
Supposons que U_i, U_j normalisent deux certains W_k et $W_{k'}$. Alors U_i, U_j sont des groupes de Klein non distingués dans $N_G\left(W_k\right)$, et $\left\langle U_i, U_j\right\rangle = N_G\left(W_k\right)$. Le même raisonnement appliqué à $W_{k'}$ donne l'égalité des deux groupes :

$$N_G\left(W_k\right) = N_G\left(W_{k'}\right)$$

On a alors que W_k et $W_{k'}$ sont deux sous-groupes isomorphes à K distingués dans $N_G\left(W_k\right) \simeq \mathfrak{S}_4$, qui est un groupe qui admet un unique sous-groupe distingué d'ordre 4. Ainsi $W_k = W_{k'}$.

Montrons maintenant par l'absurde qu'il existe un tel W_k.
Remarquons la symétrie que nous avions utilisée dans la preuve du *corollaire 2.4.14* :

$$U_i \text{ normalise } W_j \iff W_j \text{ normalise } U_i$$

Nous pouvons exploiter cette symétrie et la première partie de la preuve pour affirmer que pour tout $W_i \neq W_j$, il existe au plus un U_k qui soit normalisé par W_i et W_j (★).
Maintenant, supposons au contraire qu'il n'existe pas de W_k normalisé à la fois par U_i et U_j. Étant donné que chaque $\left\{W_k\right\}_{k\in[\![1,7]\!]}$ est normalisé par trois des $\left\{U_k\right\}_{k\in[\![1,7]\!]}$, il existe un unique W_{k_0} qui n'est normalisé ni par U_i, ni par U_j. Alors les trois des $\left\{U_k\right\}_{k\in[\![1,7]\!]}$ qui normalisent W_{k_0}, que nous appellerons $U_{k_0^{(1)}}$, $U_{k_0^{(2)}}$ et $U_{k_0^{(3)}}$, normalisent chacun un des $\left\{W_k\right\}_{k\in[\![1,7]\!]}$ qui sont normalisés par U_i ou U_j.
Nous avons déjà mis de côté cinq des $\left\{U_k\right\}_{k\in[\![1,7]\!]}$, à savoir U_i, U_j et $U_{k_0^{(1)}}$, $U_{k_0^{(2)}}$ et $U_{k_0^{(3)}}$. Les deux autres restants doivent normaliser trois des $\left\{W_k\right\}_{k\in[\![1,7]\!]}$ qui sont normalisés par U_i ou U_j.

Pour avoir le compte, cela veut dire que l'on peut exhiber une paire de $W_{k_1} \neq W_{k_2}$ qui soient normalisés par au moins deux des $\{U_k\}_{k\in[\![1,7]\!]}$ *distincts*, ce qui contredit (★).

Ainsi, il existe exactement un W_k qui soit normalisé par U_i et U_j. □

Corollaire 2.4.16. *Pour tout $W_i \neq W_j$, il existe exactement un U_k qui normalise W_i et W_j.*

Démonstration. Soient $W_i \neq W_j$.
Exploitons encore une fois la symétrie que nous avions utilisé dans la preuve du *corollaire 2.4.14* :

$$U_i \text{ normalise } W_j \iff W_j \text{ normalise } U_i$$

Par la proposition précédente, il existe exactement un U_k qui soit normalisé à la fois par W_i et par W_j. Mais alors par la même symétrie, U_k normalise à la fois W_i et W_j. □

On remarque que tout élément $g \in G$ agit par conjugaison sur les $\{U_i\}_{i\in[\![1,7]\!]}$ et les $\{U_i\}_{i\in[\![1,7]\!]}$.
Cette action, par construction, laisse stables les ensembles $\{U_i\}_{i\in[\![1,7]\!]}$ et $\{U_i\}_{i\in[\![1,7]\!]}$; et puisque la conjugaison est un automorphisme intérieur, l'action préserve la relation « être normalisé par » :

$$\forall g \in G, \quad U_i \text{ normalise } W_j \iff gU_ig^{-1} \text{ normalise } gW_jg^{-1}$$

Ce sont ces particularités, ainsi que celles données par la *proposition 2.4.13*, le *corollaire 2.4.14*, la *proposition 2.4.15* et le *corollaire 2.4.16* qui nous permettront de donner une géométrie particulière à l'ensemble des sous-groupes de Klein de G.

2.4.4 Plan de Fano, ou $\mathbb{P}^2(\mathbb{F}_2)$

La géométrie projective peut être introduite de deux façons : par les espaces vectoriels sur un corps k comme au sens de la *définition 1.3.3*, ou en utilisant des axiomes portant sur un ensemble de points et de droites, qui sont :

(A1) Par deux points distincts passe une droite et une seule.

(A2) Deux droites distinctes se coupent en un et un seul point.

(A3) Chaque droite passe par au moins 3 points.

(A4) Il existe au moins 3 points non alignés.

On s'intéresse ici au plan projectif sur $\mathbb{F}_2^3$, et nous allons étudier ses propriétés pour en déduire une autre preuve de l'unicité d'un groupe simple d'ordre 168[7][2].

Définition 2.4.17 (Plan de Fano)**.** *On appelle* plan de Fano *l'ensemble $\mathbb{P}^2(\mathbb{F}_2)$. C'est le plan projectif sur $\mathbb{F}_2^3$.*

Définition 2.4.18 (Automorphisme du plan de Fano)**.** *Un* automorphisme du plan de Fano *est une permutation des droites et des points de $\mathbb{P}^2(\mathbb{F}_2)$ préservant les propriétés précédentes. Autrement dit, si ψ est un automorphisme du plan de Fano, alors le point p appartient à la droite d si et seulement si $\psi(p)$ appartient à $\psi(d)$.*
L'ensemble des automorphisme du plan de Fano est noté Aut$(\mathbb{P}^2(\mathbb{F}_2))$*, c'est un groupe pour la composition.*

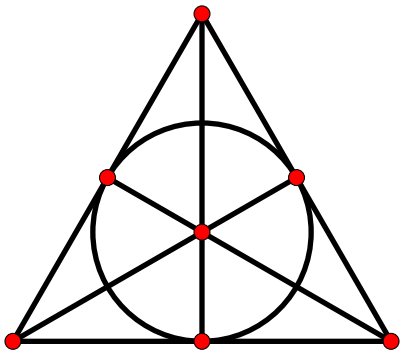
Propriétés.

- *Le plan de Fano est constitué de 7 points.*

  En effet, les « points » du plan de Fano sont les droites vectorielles de $\mathbb{F}_2^3$, et chacune de ses droites est portée par un vecteur non nul de $\mathbb{F}_2^3$, il y a $2^3 - 1 = 7$ points dans $\mathbb{P}^2(\mathbb{F}_2)$, soit 7 droites vectorielles dans $\mathbb{F}_2^3$.
- *Le plan de Fano admet 7 droites.*

  En effet, les « droites » de $\mathbb{P}^2(\mathbb{F}_2)$ sont les plans vectoriels de $\mathbb{F}_2^3$. Il sont définis par une équation $ax + by + cz = 0$, avec $a, b, c \in \mathbb{F}_2$ non tous nuls. Cette construction nous donne également 7 droites.

Plus visuellement, les points et les droites de du plan de Fano peuvent être représentés grâce au schéma suivant :



Le plan de Fano

On note alors les quelques propriétés suivantes :

Propriétés.

- *Chaque droite est constituée de trois points.*
- *Chaque point se trouve à l'intersection de trois droites.*
- *Pour chaque paire de point, il existe une unique droite passant par ces points.*
- *Pour chaque paire de droites, il existe un unique point à l'intersection de ces droites.*

Remarquons maintenant que l'on peut assimiler les $\{U_i\}_{i\in[\![1,7]\!]}$ aux points du plan de Fano et les $\{U_i\}_{i\in[\![1,7]\!]}$ aux droites du plan de Fano, et que la *proposition 2.4.13*, le *corollaire 2.4.14*, la *proposition 2.4.15* et le *corollaire 2.4.16* sont alors de parfaites reformulations des propriétés précédentes, dès que l'on remplace la relation « U_i normalise W_j » par « le point p appartient à la droite d », ou « W_j est normalisé par U_i » par « la droite d contient le point p » :

(1) Il y a 7 points et 7 droites, ainsi que 7 conjugués à U, 7 conjugués à W.

(2) Chaque W_j est normalisée par trois U_i.

(3) Chaque U_i normalise trois W_j.

(4) Pour chaque paire de U_i, il existe un unique W_j qui soient normalisés par les deux U_i.

(5) Pour chaque paire de W_j, il existe un unique U_i normalisant les deux W_j.

L'action de G sur les $\{U_i\}_{i\in[\![1,7]\!]}$ et les $\{U_i\}_{i\in[\![1,7]\!]}$ peut donc se voir comme une action d'un groupe simple d'ordre 168 sur le plan de Fano, se qui se traduit en l'existence d'un morphisme

$$\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right) \\ g & \longmapsto & \psi_g : x \longmapsto \psi_g(x) \end{array} \right.$$

où ψ_g est l'application qui à un point x, identifié à un certain U_i, associe le point identifié à gU_ig^{-1}. La remarque à la fin de la dernière partie assure que ψ_g envoie un point sur un point, une droite sur une droite, et que si p est un point d'une droite d, alors $\psi_g(p) \in \psi_g(d)$: ψ_g est donc bel et bien un automorphisme du plan de Fano.

Lemme 2.4.19. *Un groupe simple à* 168 *éléments s'identifie à un sous-groupe de* $\mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$.

Démonstration. Par simplicité de G, et puisque $\ker\varphi \lhd G$, le morphisme φ est soit injectif, soit trivial.
Montrons que φ n'est pas trivial. Les $\{U_i\}_{i\in[\![1,7]\!]}$ étant tous conjugués entre eux, il existe $g \in G$ tel que $gU_1g^{-1} = U_2 \neq U_1$. Ainsi, en appelant x_1 et x_2 les points respectivement associés à U_1 et à U_2, nous avons :

$$\varphi(g)(x_1) = \psi_g(x_1) = x_2 \neq x_1$$

Ainsi, $\varphi(g) \neq \mathrm{id}_{\mathbb{P}^2(\mathbb{F}_2)}$ et donc φ n'est pas trivial.
Le morphisme φ est donc injectif, et par le premier théorème d'isomorphisme, G est alors isomorphe à $\operatorname{im}\varphi$ qui est un sous-groupe de $\mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$. □

Lemme 2.4.20. *Le groupe d'automorphisme du plan de Fano a au plus* 168 *éléments.*

Démonstration. Montrons tout d'abord qu'un automorphisme du plan de Fano est entièrement déterminé par l'image de trois points non alignés.
Pour cela, prenons $\left(\mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{x}_3\right)$ et $\left(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3\right)$ deux triplets de points non alignés. On veut montrer qu'il existe un unique automorphisme du plan de Fano qui envoie $\left(\mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{x}_3\right)$ sur $\left(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3\right)$.

Rappelons nous que les points $\left\{\mathfrak{x}_i, \mathfrak{y}_i\right\}_{i\in[\![1,3]\!]}$ sont des droites de $\mathbb{F}_2^3$, et que chacune de ses droites comporte exactement deux vecteurs, dont un est le vecteur nul. On peut ainsi identifier chaque point $\mathfrak{x}_i, \mathfrak{y}_i$ de $\mathbb{P}^2\left(\mathbb{F}_2\right)$ avec un unique vecteur x_i, y_i non nul de $\mathbb{F}_2^3$.
Avec cette représentation, dire que les points $\mathfrak{x}_1$, $\mathfrak{x}_2$ et $\mathfrak{x}_3$ sont non alignés revient à dire que les vecteurs x_1, x_2 et x_3 ne se trouvent pas dans le même plan, et donc qu'ils forment une base de $\mathbb{F}_2^3$.
Un raisonnement analogue nous fait dire que $\left(y_1, y_2, y_3\right)$ forme une base de $\mathbb{F}_2^3$.
On considère alors $f \in \mathrm{GL}_3\left(\mathbb{F}_2\right)$ l'unique isomorphisme envoyant $\left(x_1, x_2, x_3\right)$ sur $\left(y_1, y_2, y_3\right)$. Cet endomorphisme peut alors se voir comme un automorphisme de $\mathbb{P}^2\left(\mathbb{F}_2\right)$, puisque f envoie des vecteurs non nuls sur des vecteurs non nuls, donc des droites sur des droites, et finalement établit une correspondance entre des points de $\mathbb{P}^2\left(\mathbb{F}_2\right)$. De même, l'image d'un plan de $\mathbb{F}_2^3$ est un autre plan de $\mathbb{F}_2^3$, donc f envoie les droites de $\mathbb{P}^2\left(\mathbb{F}_2\right)$ vers d'autres droites de $\mathbb{P}^2\left(\mathbb{F}_2\right)$: vu dans $\mathbb{P}^2\left(\mathbb{F}_2\right)$, f permute les points et les droites.

Il faut ensuite s'assurer que f préserve la relation d'appartenance d'un point à une droite, ce qui est le cas : si (p, d) est un couple formé d'un point et d'une droite contenant ce point, alors on peut trouver $x, y \in \mathbb{F}_2^3$ tels que $p = \mathrm{Vect}_{\mathbb{F}_2}(x)$ et $d = \mathrm{Vect}_{\mathbb{F}_2}(x, y)$. Alors $f(p) = p = \mathrm{Vect}_{\mathbb{F}_2}(f(x))$ et $f(d) = \mathrm{Vect}_{\mathbb{F}_2}(f(x), f(y))$, donc $(f(p), f(d))$ est bien un couple formé d'un point et d'une droite contenant ce point.
L'endomorphisme f peut donc être vu comme un automorphisme du plan de Fano, qui envoie $\left(\mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{x}_3\right)$ sur $\left(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3\right)$.

Pour l'unicité, il suffit de raisonner « à l'envers » ; si $\psi, \psi' \in \mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$ envoient tous les deux $\left(\mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{x}_3\right)$ sur $\left(\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3\right)$, alors la correspondance qui permet d'identifier les points de $\mathbb{P}^2\left(\mathbb{F}_2\right)$ et les vecteurs non nuls de $\mathbb{F}_2^3$ nous affirme que ψ et ψ' envoient tous deux une base sur une autre, il s'agit donc du même automorphisme.

Maintenant, étant donné un triplet de points non alignés de $\mathbb{P}^2\left(\mathbb{F}_2\right)$, on remarque qu'il y a 7 choix possibles pour l'image du premier élément. Le deuxième ne peut être envoyé sur le premier, il reste donc 6 choix pour l'image du deuxième. Les images des deux premiers points se trouvent sur une même et unique droite d, et le dernier point doit être envoyé sur un point extérieur à d. Une droite étant constituée de trois points, il y a 4 choix possibles pour l'image du troisième point.
Ainsi, $\mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$ a au plus $7 \cdot 6 \cdot 4 = 168$ éléments. □

Théorème 2.4.21 (Unicité d'un groupe simple d'ordre 168)**.** *Un groupe simple d'ordre* 168 *est isomorphe au plan de Fano et est donc unique.*

Démonstration. Nous savons que si G est un groupe simple d'ordre 168 alors G s'identifie à un sous-groupe de $\mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$, qui est de cardinal au plus 168 par le lemme précédent. Par égalité des ordres, nous avons :

$$G \simeq \mathrm{Aut}\left(\mathbb{P}^2\left(\mathbb{F}_2\right)\right)$$

□

3 Table des caractères du groupe simple d'ordre 168

3.1 Représentation par permutation

3.1.1 Définitions et résultats

Dans cette sous-partie nous parlerons de résultats généraux sur la *représentation par permutation*, ainsi G désignera ici un groupe fini quelconque, sauf mention du contraire.

Soit E un ensemble fini et G un groupe agissant sur E par :

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

On pose $\mathbb{C}[E] \overset{\text{def}}{=} \mathbb{C}^E = \{f : E \longrightarrow \mathbb{C}\}$. On a alors :

Théorème 3.1.1. *Le groupe G agit sur $\mathbb{C}[E]$ par :*

$$\begin{array}{ccccc} G \times \mathbb{C}[E] & \longrightarrow & \mathbb{C}[E] & & \\ (g, f) & \longmapsto & g\star f : & \left\{ \begin{array}{ccc} E & \longrightarrow & \mathbb{C} \\ x & \longmapsto & f\left(g^{-1} \cdot x\right) \end{array} \right. \end{array}$$

Démonstration. Soit $f \in \mathbb{C}[E]$. Pour tout $x \in E$, on a $\left(1_G \star f\right)(x) = f\left(1_G^{-1} \cdot x\right) = f(x)$ car G agit sur E, ainsi $1_G \star f = f$.
Soient $g, g' \in G$ et $f \in \mathbb{C}[E]$. Alors pour tout $x \in E$ nous avons :

$$\begin{aligned} \left(g' \star (g \star f)\right)(x) &= (g \star f)\left(g'^{-1} \cdot x\right) \\ &= f\left(g^{-1} \cdot \left(g'^{-1} \cdot x\right)\right) \\ &= f\left(\left(g'g\right)^{-1} \cdot x\right) \\ &= \left(\left(g'g\right) \star f\right)(x) \end{aligned}$$

Ainsi $g' \star (g \star f) = \left(g'g\right) \star f$, le groupe G agit donc sur $\mathbb{C}[E]$. □

De plus, cette action est une action linéaire, c'est-à-dire que pour toutes fonctions $f_2, f_2 \in \mathbb{C}[E]$ et $\lambda \in \mathbb{C}$, nous avons :

$$\forall \in G, \quad g\star\left(\lambda f_1 + f_2\right) = \lambda\left(g \star f_1\right) + g \star f_2$$

Autrement dit, le morphisme $G \longrightarrow \mathfrak{S}(\mathbb{C}[E])$ induit par l'action de G sur $\mathbb{C}[E]$ s'injecte en réalité dans $\mathrm{GL}(\mathbb{C}[E])$, ce qui motive la définition suivante :

Définition 3.1.2 (Représentation par permutation)**.** *Si on note ϱ le morphisme induit par l'action de G sur $\mathbb{C}[E]$, alors le couple $(\mathbb{C}[E], \varrho)$ est une représentation de G, appelée* représentation par permutation.

Notation. *Si $x \in E$, on posera $e_x \in \mathbb{C}[E]$ l'application :*

$$e_x = \mathbb{1}_{\{x\}} : x' \longmapsto \delta_{xx'}$$

Propriété. *Pour tout $g \in G$ et $x \in E$, on a $g \star e_x = e_{g \cdot x}$.*

En effet, un simple calcul montre que pour tout $x' \in E$, on a :

$$\begin{aligned} \left(g \star e_x\right)(x') &= e_x\left(g^{-1} \cdot x'\right) \\ &= \delta_{x\, g^{-1} \cdot x'} \\ &= \delta_{g \cdot x\, x'} \\ &= e_{g \cdot x}(x') \end{aligned}$$

Notations.

- *Nous noterons* $\mathbb{C}[E]^G$ *l'ensemble des points fixes de* $\mathbb{C}[E]$ *sous l'action de* G*, c'est-à-dire que l'on a :*

$$\mathbb{C}[E]^G \overset{def}{=} \{ f \in \mathbb{C}[E] \mid g\star f = f \}$$

- *Nous noterons* $\mathbb{C}[E]_G$ *l'ensemble suivant :*

$$\mathbb{C}[E]_G \overset{def}{=} \left\{ f \in \mathbb{C}[E] \;\middle|\; \sum_{g\in G} g\star f = 0 \right\}$$

Remarquons maintenant que si $f \in \mathbb{C}[E]$, alors nous avons :

$$f = \underbrace{\frac{1}{|G|}\sum_{g\in G} g\star f}_{\in \mathbb{C}[E]^G} + \underbrace{\left(f - \frac{1}{|G|}\sum_{g\in G} g\star f \right)}_{\in \mathbb{C}[E]_G}$$

En effet, pour tout $g' \in G$, la multiplication par g' à gauche dans G étant une bijection, et l'action de G sur $\mathbb{C}[E]$ étant linéaire nous avons que :

$$g'\star\left(\frac{1}{|G|}\sum_{g\in G} g\star f\right) = \frac{1}{|G|}\sum_{g\in G}(g'g)\star f = \frac{1}{|G|}\sum_{g\in G} g\star f$$

Ainsi la partie de gauche est bien un point fixe sous l'action de G. Pour la partie de droite, il suffit de constater que :

$$\begin{aligned}\sum_{g'\in G} g'\star\left(f - \frac{1}{|G|}\sum_{g\in G} g\star f\right) &= \sum_{g'\in G} g'\star f - \sum_{g'\in G}\left(\frac{1}{|G|}\sum_{g\in G}(g'g)\star f\right)\\ &= \sum_{g\in G} g\star f - \sum_{g'\in G}\left(\frac{1}{|G|}\sum_{g\in G} g\star f\right)\\ &= \sum_{g\in G} g\star f - \frac{|G|}{|G|}\sum_{g\in G} g\star f = 0\end{aligned}$$

La partie de droite appartient donc bien à $\mathbb{C}[E]_G$. De plus, si $f \in \mathbb{C}[E]^G \cap \mathbb{C}[E]_G$, alors :

$$\sum_{g\in G} g\star f = \sum_{g\in G} f = |G| f = 0$$

Il en découle que $f = 0$, et ainsi :

$$\mathbb{C}[E] = \mathbb{C}[E]^G \oplus \mathbb{C}[E]_G \qquad (\clubsuit)$$

Propriété. *La famille* $\left(e_x\right)_{x\in E}$ *forme une base de* $\mathbb{C}[E]$.

En effet, on rappelle que les $\left(e_x\right)_{x\in E}$ sont les indicatrices des singletons de E, ainsi chaque fonction $f \in \mathbb{C}[E]$ admet une unique écriture :

$$f = \sum_{x\in E} f(x)\mathbb{1}_{\{x\}} = \sum_{x\in E} f(x) e_x$$

Cela a pour conséquence immédiate que $\dim_{\mathbb{C}} \mathbb{C}[E] = |E|$.

Constatons maintenant que $\mathbb{C}[E]^G$ contient exactement les applications f constantes sur les orbites de l'action de G sur E. D'une part, si l'on désigne par Ω l'ensemble de ces orbites, que x_ω est un des éléments de $\omega \in \Omega$, alors une application f constante sur les orbites s'écrit de manière unique sous la forme :

$$f = \sum_{\omega\in\Omega} f\left(x_\omega\right)\mathbb{1}_\omega \qquad (\heartsuit)$$

On constate alors que, pour tout $\omega \in \Omega$ on a :

$$\mathbb{1}_\omega = \sum_{x\in\omega} e_x \qquad \text{et pour tout } g \in G, \quad g\bigstar \mathbb{1}_\omega = \sum_{x\in\omega} e_{g\cdot x} = \sum_{x\in\omega} e_x = \mathbb{1}_\omega$$

Ainsi $f \in \mathbb{C}[E]^G$.

Réciproquement, si $f \in \mathbb{C}[E]^G$ alors pour tout $g \in G$ nous avons que :

$$f - g^{-1}\bigstar f = 0 = \sum_{x\in E} \left(f(x) - f\left(g\cdot x\right)\right) e_x$$

Les $(e_x)_{x\in E}$ formant une base de $\mathbb{C}[E]$, nous avons que $f(x) = f(g\cdot x)$ pour tout $x \in E$. Ceci étant vrai pour tout $g \in G$, nous avons que f est constante sur les orbites de l'action de G sur E.

Nous avons aussi obtenu de (♥) que les $\left(\mathbb{1}_\omega\right)_{\omega\in\Omega}$ forment une base de $\mathbb{C}[E]^G$, en conséquence nous avons $\dim_{\mathbb{C}} \mathbb{C}[E]^G = |\Omega|$, et donc de (♣) on tire alors que $\dim_{\mathbb{C}} C[E]_G = |E| - |\Omega|$.

Ayant exhibé une base $\mathbb{C}[E]$, à savoir $\mathfrak{b} = \left(e_x\right)_{x\in E}$, nous voulons en connaître un peu plus sur les caractères de la représentation par permutation.

Propriétés.

- *Si $g \in G$, alors :*
$$\chi_{\mathbb{C}[E]}(g) = |\operatorname{Fix}(g)|$$
En effet, si on note ϱ le morphisme de G dans $\mathrm{GL}_{|E|}(\mathbb{C})$ associé à la représentation par permutation, en se souvenant que $g\bigstar e_x = e_{g\cdot x}$ pour tout $x \in E$, il vient alors que $\varrho(g)$ est un automorphisme dont la matrice dans la base $\mathfrak{b}$ est :
$$M(g) \overset{def}{=} \operatorname{Mat}\left(\varrho(g), \mathfrak{b}\right) = \left(\delta_{x\, g\cdot x'}\right)_{x,x'\in E}$$
Ainsi nous avons :
$$\chi_{\mathbb{C}[E]}(g) = \operatorname{tr} M(g) = |\{x \in E \mid g\cdot x = x\}| = |\operatorname{Fix}(g)|$$
- *Pour tout $g \in G$, nous avons :*
$$\chi_{\mathbb{C}[E]^G}(g) = |\Omega|$$
Cela vient du fait que si on note $\varrho' : G \longrightarrow \mathrm{GL}_{|\Omega|}(\mathbb{C})$ le morphisme associé à la représentation $\mathbb{C}[E]^G$, et si l'on pose $g\cdot\omega = \{g\cdot x \mid x \in \omega\}$ pour $\omega \in \Omega$, alors l'endomorphisme $\varrho'(g)$ a pour matrice dans la base $\mathfrak{b}' = \left(\mathbb{1}_\omega\right)_{\omega\in\Omega}$
$$M'(g) = \operatorname{Mat}\left(\varrho', \mathfrak{b}'\right) = \left(\delta_{\omega\, g\cdot\omega'}\right)_{\omega,\omega'\in\Omega} = \mathrm{I}_{|\Omega|}$$
qui a bien $|\Omega|$ pour trace.
- *Pour tout $g \in G$, on a :*
$$\chi_{\mathbb{C}[E]_G}(g) = |\operatorname{Fix}(g)| - |\Omega|$$
Cela provient simplement du calcul des caractères $\chi_{\mathbb{C}[E]}$ et $\chi_{\mathbb{C}[E]^G}$, et de la somme directe $\mathbb{C}[E] = \mathbb{C}[E]^G \oplus \mathbb{C}[E]_G$.

Remarque. *La représentation par permutation tire son nom du fait que si $g \in G$, alors $\varrho(g)$ est un automorphisme dont la matrice dans la base $\mathfrak{b}$ est exactement une matrice de permutation.*

On a déjà scindé la représentation par permutation en deux sous-représentations grâce à (♣), on aimerait alors bien savoir si ces deux sous-représentations sont irréductibles ou non. Pour cela, nous avons le théorème suivant :

Théorème 3.1.3. *Si G agit doublement transitivement sur E, alors la représentation $\mathbb{C}[E]_G$ est irréductible.*
Dans ce cas, la représentation $\mathbb{C}[E]_G$ est de degré $|E| - 1$.

Démonstration. Si G agit 2-transitivement sur E, alors en particulier G agit transitivement sur E, donc l'action de G sur E n'a qu'une seule orbite, ce permet de dire que si $g \in G$ alors

$$\chi_{\mathbb{C}[E]_G}(g) = |\operatorname{Fix}(g)| - 1$$

Remarquons alors que $\operatorname{Fix}(g) = \operatorname{Fix}\left(g^{-1}\right)$ puisque pour tout $x \in E$, on a

$$g \cdot x = x \iff x = g^{-1} \cdot x$$

On calcule alors, avec le produit hermitien des caractères :

$$\begin{aligned}\left\langle \chi_{\mathbb{C}[E]_G}, \chi_{\mathbb{C}[E]_G} \right\rangle &= \frac{1}{|G|} \sum_g \chi_{\mathbb{C}[E]_G}(g)\overline{\chi_{\mathbb{C}[E]_G}}(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} (|\operatorname{Fix}(g)| - 1)^2 \\ &= \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|^2 - \frac{2}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)| + 1\end{aligned}$$

Par la formule de Burnside, nous avons :

$$1 = |\Omega| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$$

Le fait que l'action de G sur E soit doublement transitive nous donne que l'action de G sur $E \times E$ admet deux orbites :

$$\omega_1 = \{(x, x) \mid x \in E\} \qquad \text{et} \qquad \omega_2 = \{(x, y) \mid x, y \in E,\ x \neq y\}$$

On veut ainsi appliquer la formule de Burnside à cette action. Si $g \in G$, notons $\operatorname{Fix}_2(g)$ le fixateur de g sous l'action sur $E \times E$, et on conserve la notation $\operatorname{Fix}(g)$ pour l'action de G sur E. On remarque alors :

$$\operatorname{Fix}_2(g) = \{(x, y) \in E \mid g \cdot x = x \text{ et } g \cdot y = y\} = \operatorname{Fix}(g) \times \operatorname{Fix}(g)$$

Cela nous donne :

$$2 = |\Omega_{E \times E}| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_2(g)| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|^2$$

Ainsi, on a :

$$\left\langle \chi_{\mathbb{C}[E]_G}, \chi_{\mathbb{C}[E]_G} \right\rangle = 2 - 2 \cdot 1 + 1 = 1$$

On sait que ce calcul caractérise l'irréductibilité, ainsi la représentation $\mathbb{C}[E]_G$ est bien irréductible. □

Remarque. *En réalité nous avons même la réciproque dans le* théorème 3.1.3 *: si G agit transitivement sur E, alors :*

G agit doublement transitivement sur $E \iff \mathbb{C}[E]_G$ est irréductible

Toutefois, notre objectif étant d'exhiber des représentations irréductibles, nous n'aurons besoin que du sens direct.

Nous allons pouvoir rechercher les représentations du groupe simple d'ordre 168.

3.1.2 Représentation de degré 6

Reprenons G le groupe simple à 168 éléments. Nous pouvons le voir comme $\mathrm{GL}_3(\mathbb{F}_2) = \mathrm{PSL}_3\left(\mathbb{F}_2\right)$.

On sait que les groupes spéciaux projectifs linéaires agissent doublement transitivement sur l'ensemble des droites vectorielles [11], ainsi le G agit doublement transitivement sur les droites de $\mathbb{F}_2^3$, c'est-à-dire que G agit 2-transitivement sur $\mathbb{P}^2\left(\mathbb{F}_2\right)$.

En vertu du *théorème 3.1.3*, nous avons que la représentation par permutation $\mathbb{C}\left[\mathbb{P}^2\left(\mathbb{F}_2\right)\right]_{\mathrm{PSL}_3(\mathbb{F}_2)}$ est irréductible.

11. Voir *page 26* le lemme intermédiaire dans la preuve du *théorème 1.2.9*.

Cette représentation est de degré $\left|\mathbb{P}^2\left(\mathbb{F}_2\right)\right| - 1 = 7 - 1 = 6$, et nous noterons χ_6 le caractère associé.

Nous savons que pour tout $g \in G$, $\chi_6(g) = |\operatorname{Fix}(g)| - 1$, et que la valeur des caractères est la même sur chaque classe de conjugaison du groupe G, nous calculerons ainsi ces caractères pour des représentants bien choisis de chaque classe.

En nous rappelant que $g \in G$ est un automorphisme de $\mathbb{F}_2^3$, nous avons que la seule valeur propre que g puisse admettre est 1, ainsi une droite $d = \operatorname{Vect}_{\mathbb{F}_2}(v)$ avec $v \in \mathbb{F}_2^3 \setminus \{0\}$ est fixe si et seulement si $g(v) = v$, c'est-à-dire si et seulement si $d \subseteq \ker(g - \mathrm{id})$.

Notons $n = \ker(g - \mathrm{id})$, et prenons $(e_1, \cdot, e_n)$ une base de $\ker(g - \mathrm{id})$. Un vecteur de $\ker(g - \mathrm{id})$ s'écrit donc

$$\lambda_1 e_1 + \cdot + \lambda_n e_n$$

avec $\lambda_1, \cdot, \lambda_n \in \mathbb{F}_2$. En particulier nous avons alors 2^n choix possibles pour le n-uplet $\left(\lambda_1, \cdot, \lambda_n\right)$, et un seul correspond au vecteur nul.

Puisque nous sommes sur $\mathbb{F}_2$, il y a une correspondance bijective entre les droites vectorielles de $\mathbb{F}_2^3$ et les vecteurs non nuls de F_2^3, ainsi $\ker(g - \mathrm{id})$ contient exactement $2^n - 1$ droites.

Propriété. *Si $g \in G$, alors il y a exactement $2^{\dim_{F_2}(\ker(g-\mathrm{id}))} - 1$ droites stables par g.*

Cela nous donne la formule suivante pour les caractères de la représentation de degré 6 :

$$\forall g \in G, \quad \chi_6(g) = 2^{\dim_{F_2}(\ker(g-\mathrm{id}))} - 2$$

Effectuons ce calcul pour des représentant de chaque classe :

- Ordre 1 : si $g \in G$ est d'ordre 1, on sait que $g = \mathrm{I}_3$ et $\chi_6(g) = 6$, ce qu'on peut retrouver puisque $\ker(g - \mathrm{I}_3)$ est alors de dimension 3, ce qui donne par la formule précédente que $\chi_6(g) = 2^3 - 2 = 6$.
- Ordre 2 : pour $g \in G$ d'ordre 2, on peut prendre :

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Alors $g - \mathrm{I}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ dont le noyau est de dimension 2, ce qui nous donne un caractère :

$$\chi_6(g) = 2^2 - 2 = 2$$

- Ordre 3 : de la même manière, pour l'ordre 3, on peut prendre

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

ce qui nous donne $g - \mathrm{I}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ de rang 2 donc $\dim_{\mathbb{F}_2}\left(\ker(g - \mathrm{I}_3)\right) = 1$, et alors :

$$\chi_6(g) = 2^1 - 2 = 0$$

- Ordre 4 : un représentant de la classe d'ordre 4 est

$$g = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

donc $g - \mathrm{I}_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ qui est aussi de rang 2, on a donc également :

$$\chi_6(g) = 2^1 - 2 = 0$$

• Ordre 7 : il y a deux classes d'ordre 7, mais les éléments d'une classe sont les inverses des éléments de l'autre classe. Ainsi dire que g d'ordre 7 fixe une droite d, disons $d = \mathrm{Vect}_{\mathbb{F}_2}(v)$ pour $v \in \mathbb{F}_2^3$ un certain vecteur non nul, cela revient à dire que $g(v) = v$, mais alors $v = g^{-1}(v)$ et donc g^{-1} stabilise exactement les mêmes droites que g.
Ainsi les éléments des deux classes laissent invariants exactement le même nombre de droites, et ont donc exactement le même caractère.
On se donne donc g un élément d'ordre 7, disons :

$$g = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Alors $g - \mathrm{I}_3 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ qui est inversible, donc de noyau trivial. Ainsi nous avons :

$$\chi_6(g) = \chi_6\left(g^{-1}\right) = 2^0 - 2 = -1$$

Nous avons donc :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_6	6	2	0	0	-1	-1

3.1.3 Représentation de degré 7

Le groupe simple à 168 éléments peut également être vu comme $\mathrm{PSL}_2\left(\mathbb{F}_7\right)$ qui agit doublement transitivement sur les droites vectorielles de $\mathbb{F}_7^2$, c'est-à-dire que G agit 2-transitivement sur $\mathbb{P}^1\left(\mathbb{F}_7\right)$, nous avons donc une représentation irréductible de degré $\left|\mathbb{P}^1\left(\mathbb{F}_7\right)\right| - 1 = 8 - 1 = 7$ donnée par $\mathbb{C}\left[\mathbb{P}^1\left(\mathbb{F}_7\right)\right]_{\mathrm{PSL}_2(\mathbb{F}_7)}$.
Nous noterons χ_7 le caractère associé à cette représentation.

Avant de calculer les caractères de cette représentation, il nous faut établir à quoi ressemblent les classes de conjugaison du point de vue $\mathrm{PSL}_2\left(\mathbb{F}_7\right)$.

Des représentants respectifs de la classe d'ordre 1, 2, 3, 4 et des deux classes d'ordre 7 sont donnés par :

$$g_1 = \overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \quad g_2 = \overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}} \quad g_3 = \overline{\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}} \quad g_4 = \overline{\begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix}} \quad g_7 = \overline{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}} \quad g_7^{-1} = \overline{\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}}$$

où $\overline{f}$ désigne la classe de l'endomorphisme $f \in \mathrm{SL}_2\left(\mathbb{F}_7\right)$ dans le quotient $\mathrm{PSL}_2\left(\mathbb{F}_7\right) = \mathrm{SL}_2\left(\mathbb{F}_7\right) / \left\{\pm \mathrm{I}_2\right\}$. On vérifie aisément alors que g_i est d'ordre i pour $i \in \{1, 2, 3, 4, 7\}$ et que ce sont bien des éléments de $\mathrm{PSL}_2\left(\mathbb{F}_7\right)$.

Nous voulons maintenant calculer les caractères de cette représentation. Pour cela il nous faut déterminer, pour chaque représentant de chaque classe, le nombre de droites stables.

• Ordre 1 : le caractère de la classe d'ordre 1 valant le degré de la représentation, nous avons $\chi_7(g_1) = 7$, ce que nous retrouvons puisque g_1 stabilise tout $\mathbb{P}^1\left(\mathbb{F}_7\right)$.

• Ordre 2 : pour g_2, on regarde un endomorphisme de $\mathrm{SL}_2\left(\mathbb{F}_7\right)$ envoyé sur g_2 par passage au quotient : on regarde $f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ qui a pour polynôme caractéristique $X^2 + 1 = X^2 - 6$.
Or $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^4 = 2$ et $6^2 = 1$, donc 6 n'est pas un carré dans $\mathbb{F}_7$, et donc f n'admet pas de valeurs propres, donc $\mathrm{Fix}(g_2) = \varnothing$ et :

$$\chi_7(g_2) = 0 - 1 = -1$$

• Ordre 3 : de même, pour g_3, on regarde $f = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$ et on s'aperçoit alors que f stabilise exactement les deux droites $\mathrm{Vect}_{\mathbb{F}_7}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\mathrm{Vect}_{\mathbb{F}_7}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, donc $|\mathrm{Fix}(g_3)| = 2$ et on a :

$$\chi_7(g_3) = 2 - 1 = 1$$

• Ordre 4 : prenons $f = \begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix}$ qui est envoyé sur g_4 dans le quotient $\mathrm{PSL}_2\left(\mathbb{F}_7\right)$. L'endomorphisme f a pour polynôme caractéristique $(X-2)^2+2 = X^2+3X-1$ qui n'admet pas de racines dans $\mathbb{F}_7$. Ainsi $\mathrm{Fix}(g_4) = \varnothing$ et :

$$\chi_7(g_4) = 0 - 1 = -1$$

• Ordre 4 : remarquons à nouveau que g_7 et g_7^{-1} stabiliserons les mêmes droites, ainsi on peut calculer le fixateur de g_7 seulement. On étudie $f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de polynôme caractéristique $(X-1)^2$ qui admet 1 comme racine, ainsi f admet une valeur propre.

Ainsi si f stabilise une droite $d = \mathrm{Vect}_{\mathbb{F}_7}\begin{pmatrix} x \\ y \end{pmatrix}$ alors :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{c'est-à-dire} \quad \begin{pmatrix} x+y \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Donc $y = 0$ et nous avons nécessairement que $d = \mathrm{Vect}_{\mathbb{F}_7}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et f ne stabilise donc qu'une seule droite, ce qui nous donne :

$$\chi_7(g_7) = \chi_7\left(g_7^{-1}\right) = 1 - 1 = 0$$

En résumé, nous avons :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_7	7	−1	1	−1	0	0

3.2 Représentation de degré 8

Nous avons déjà obtenu une représentation de degré 6 et une de degré 7, irréductibles, dont nous avons calculé les caractères.

Reprenons G le groupe simple d'ordre 168 et choisissons de le voir comme $\mathrm{GL}_3\left(\mathbb{F}_2\right)$. Posons $\mathscr{D}$ l'ensemble des droites de $\mathbb{F}_2^3$ et $\mathscr{P}$ l'ensemble des plans de $\mathbb{F}_2^3$.
On pose alors $E = \{(d,p) \in \mathscr{D} \times \mathscr{P} \mid d \subseteq p\}$.

Dans $\mathbb{F}_2^3$, un plan est caractérisé par son vecteur normal (il est unique en caractéristique 2), et il y a $2^3 - 1 = 7$ vecteurs non nuls dans $\mathbb{F}_2^3$, donc $|\mathscr{P}| = 7$. Chacun de ses plans est engendré par deux vecteurs non nuls, disons $\mathscr{P} \ni p = \mathrm{Vect}_{\mathbb{F}_2}(u,v)$, $u, v \in \mathbb{F}_2^3 \setminus \{0\}$. On a alors :

$$p = \{0, u, v, u+v\}$$

qui contient exactement trois vecteurs non nuls, et donc contient trois droites de $\mathscr{D}$. Ainsi $|E| = 3 \cdot 7 = 21$.

Propriété. *le groupe G agit sur E par l'action :*

$$\begin{array}{rcl} G \times E & \longrightarrow & E \\ (g,(d,p)) & \longmapsto & g * (d,p) \overset{def}{=} (g \cdot d, g \cdot p) \end{array}$$

où $g \cdot d$, $g \cdot p$ désignent l'image de d et de p par l'automorphisme $g \in GL_3\left(\mathbb{F}_2\right)$.

En effet, il est clair que pour $(d,p) \in E$, $\mathrm{id} * (d,p) = (d,p)$, et que si $g, g' \in \mathrm{GL}_3\left(\mathbb{F}_2\right)$, alors :

$$\begin{aligned} g' * (g * (d,p)) &= g' * (g \cdot d, g \cdot p) \\ &= \left((g' \circ g) \cdot d, (g' \circ g) \cdot p\right) \\ &= (g'g) * (d,p) \end{aligned}$$

Ainsi G agit sur E.

La représentation par permutation $\mathbb{C}[E]$ donne alors une représentation de G de degré $|E| = 21$, et pour tout $g \in G$, le caractère $\chi_{\mathbb{C}[E]}(g)$ vaut $|\mathrm{Fix}(g)|$, on veut donc calculer les fixateurs des éléments de g.

Commençons par énumérer les plans de $\mathscr{P}$, en prenant la convention d'écriture désignant les coordonnées d'un vecteur de $\mathbb{F}_2^3$ par (x, y, z) :

$$p_1 = \{x = 0\} \quad p_2 = \{y = 0\} \quad p_3 = \{z = 0\} \quad p_4 = \{x+y = 0\} \quad p_5 = \{x+z = 0\} \quad p_6 = \{y+z = 0\} \quad p_7 = \{x+y+z = 0\}$$

Autrement, nous avons :

$$p_1 = \text{Vect}\left(\begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right) \quad p_2 = \text{Vect}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right) \quad p_3 = \text{Vect}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}\right)$$

$$p_4 = \text{Vect}\left(\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right) \quad p_5 = \text{Vect}\left(\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right) \quad p_6 = \text{Vect}\left(\begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right) \quad p_7 = \text{Vect}\left(\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}\right)$$

On remarque que si g laisse fixe $(d, p) \in E$ et que $u \in \mathbb{F}_2^3$ est tel que $d = \text{Vect}_{\mathbb{F}_2}(u)$, alors $(g - \mathrm{I}_3)(u) = 0$.

De plus, si $v \in \mathbb{F}_2^3$ est tel que $p = \text{Vect}_{\mathbb{F}_2}(u, v)$, alors $g(v) \in \{v, u + v\}$. En effet, p étant laissé stable par g, $g(v)$ est un des éléments de p, c'est-à-dire qu'à priori $g(v) \in \{0, u, v, u + v\}$, mais v ne peut en réalité par être envoyé sur le vecteur nul par g car g est inversible, et ne peut être envoyé sur u sinon l'image de p par g serait la droite d qui n'est pas de dimension 2.

Cela nous donne que $(g - \mathrm{I}_3)(v) \in \{0, v\}$, et alors $(g - \mathrm{I}_3)^2(v) = 0$, d'où :

Propriété. *Si $g \in G$ fixe $(d, p) \in E$, alors $d \subseteq p \subseteq \ker(g - \mathrm{I}_3)^2$.*

Nous pouvons alors calculer les caractères de la représentation $\mathbb{C}[E]$.

- Ordre 1 : pour g d'ordre 1, nous avons $\chi_{\mathbb{C}[E]}(g) = \deg \mathbb{C}[E] = 21$.
- Ordre 2 : un représentant de la classe d'ordre 2 est donné par :

$$g = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}$$

Supposons $d = \text{Vect}_{\mathbb{F}_2}(v)$ soit une droite stable par g. En notant x, y et z les coordonnées de v, nous avons :

$$\begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\y\\z\end{pmatrix} \iff \begin{cases} x &= x\\ y+z &= y\\ z &= z\end{cases} \iff z = 0$$

Il y a ainsi trois vecteurs propres pour g :

$$v_1 \overset{\text{def}}{=} \begin{pmatrix}1\\0\\0\end{pmatrix} \qquad v_2 \overset{\text{def}}{=} \begin{pmatrix}0\\1\\0\end{pmatrix} \qquad v_3 \overset{\text{def}}{=} \begin{pmatrix}1\\1\\0\end{pmatrix}$$

On remarque que tous les plans contiennent au moins un de ces vecteurs, il va donc falloir déterminer « à la main » quels sont les plans stables par g.

▷ p_1 : le premier plan contient trois vecteurs non nuls : les deux vecteurs que nous avons donné pour engendrer p_1 (voir la liste des plans de $\mathbb{F}_2^3$ à la *page 53*) et la somme des deux. On calcule alors les images des ces vecteurs par g :

$$\begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix} \qquad \begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\1\end{pmatrix} \qquad \begin{pmatrix}1 & 0 & 0\\0 & 1 & 1\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix}$$

On remarque que les images des vecteurs non nuls de p_1 sont exactement les vecteurs non nuls de p_1, ainsi $g \cdot p_1 = p_1$ et p_1 est stable par g.

Le vecteur v_1 étant le seul vecteur non nul stable par g, nous avons obtenu que $\left(\text{Vect}_{\mathbb{F}_2}(v_1), p_1\right) \in \text{Fix}(g)$.

▷ p_2 : passons un peu les calculs qui sont similaires au cas précédent. Nous avons les trois vecteurs non nuls de p_2, et nous calculons leurs images ce qui nous donne exactement les vecteurs non nuls de p_6.

Ainsi $g \cdot p_2 = p_6 \neq p_2$: p_2 n'est pas stable par g.

▷ p_3 : cette fois-ci, on remarque que tous les vecteurs non nuls de p_3 sont exactement les vecteurs non nuls qui ont leur dernière coordonnée nulle, c'est-à-dire $p_3 = \{0, v_1, v_2, v_3\}$ où v_1, v_2 et v_3 sont stables par g ; donc non seulement p_3 est stable par g, mais aussi $g_{|p_3} = \mathrm{id}_{p_3}$ et nous obtenons ainsi trois couples de E stables par g :

$$\left(\mathrm{Vect}_{\mathbb{F}_2}(v_1), p_3\right), \left(\mathrm{Vect}_{\mathbb{F}_2}(v_2), p_3\right), \left(\mathrm{Vect}_{\mathbb{F}_2}(v_3), p_3\right) \in \mathrm{Fix}(g)$$

▷ p_4 : on calcule les images des vecteurs non nuls de p_4, ce qui nous donne les vecteurs non nuls de p_7. Le plan p_4 n'est donc pas stable par g.

▷ p_5 : calculons :

$$\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix} \quad \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}=\begin{pmatrix}0\\1\\0\end{pmatrix} \quad \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\0\end{pmatrix}$$

Les images sont les vecteurs non nuls de p_5, ainsi p_5 est stable par g, et il ne contient qu'une seule droite stable par g, engendrée par v_2, ainsi $\left(\mathrm{Vect}_{\mathbb{F}_2}(v_2), p_5\right) \in \mathrm{Fix}(g)$.

▷ p_6 : nous avions calculé que $g \cdot p_2 = p_6$. Puisque g est d'ordre 2, nous avons $g \cdot p_6 = g^2 \cdot p_2 = p_2 \neq p_6$, ainsi p_6 n'est pas stable par g.

▷ p_7 : de la même manière, nous avions déterminé que $g \cdot p_4 = p_7$, donc $g \cdot p_7 = p_4 \neq p_7$ et p_7 n'est pas stable par g.

Après avoir énuméré tous les cas, nous avons obtenu au total cinq éléments de E fixes par g, ainsi :

$$\chi_{\mathbb{C}[E]}(g) = 5$$

• Ordre 3 : prenons :

$$g = \begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}$$

Alors $\left(g - \mathrm{I}_3\right)^2 = \begin{pmatrix}0&0&0\\0&1&1\\0&1&0\end{pmatrix}^2 = \begin{pmatrix}0&0&0\\0&0&1\\0&1&1\end{pmatrix}$ qui a un noyau de dimension 1, et donc ne contient aucun plan. Moralité : par la propriété précédente, g ne peut fixer aucun élément de E, donc :

$$\chi_{\mathbb{C}[E]}(g) = |\,\mathrm{Fix}(g)| = 0$$

• Ordre 4 : prenons cette fois-ci :

$$g = \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

donc $\left(g - \mathrm{I}_3\right)^2 = \begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}^2 = \begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}$ de noyau de dimension 2, donc qui contient exactement un plan. On vérifie que ce plan est p_3 ($\{z = 0\}$), et il nous maintenant déterminer les droites de p_3 fixées par g. Les trois droites de p_3 sont les droites :

$$d_1 \overset{\text{def}}{=} \mathrm{Vect}_{\mathbb{F}_2}\begin{pmatrix}1\\0\\0\end{pmatrix} \quad d_2 \overset{\text{def}}{=} \mathrm{Vect}_{\mathbb{F}_2}\begin{pmatrix}0\\1\\0\end{pmatrix} \quad d_3 \overset{\text{def}}{=} \mathrm{Vect}_{\mathbb{F}_2}\begin{pmatrix}1\\1\\0\end{pmatrix}$$

Or :

$$\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix} \quad \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}=\begin{pmatrix}1\\1\\0\end{pmatrix}\neq\begin{pmatrix}0\\1\\0\end{pmatrix} \quad \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\0\end{pmatrix}\neq\begin{pmatrix}1\\1\\0\end{pmatrix}$$

Il n'y a donc qu'une seule droite de p_3 fixée par g, donc $\mathrm{Fix}(g) = \left\{\left(d_1, p_3\right)\right\}$, d'où :

$$\chi_{\mathbb{C}[E]}(g) = 1$$

• Ordre 7 : si g est d'ordre 7, on sait que ni g ni g^{-1} ne fixent de droites, et en particulier aucun des deux ne peut alors fixer d'élément de E, d'où :

$$\chi_{\mathbb{C}[E]}(g) = \chi_{\mathbb{C}[E]}\left(g^{-1}\right) = 0$$

En résumé, nous avons :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
$\chi_{\mathbb{C}[E]}$	21	5	0	1	0	0

Nous voulons maintenant casser cette représentation en sous-représentation irréductibles.

L'ensemble des caractères irréductibles forme une base orthonormée de l'ensemble des caractères, ainsi, en notant $\mathscr{X}$ l'ensemble des caractères irréductibles de G, nous avons :

$$\chi_{\mathbb{C}[E]} = \sum_{\chi \in \mathscr{X}} \left\langle \chi, \chi_{\mathbb{C}[E]} \right\rangle \chi$$

Dans $\mathscr{X}$, nous savons qu'il y a χ_0 le caractère de la représentation triviale, χ_6 et χ_7, dont nous avons calculé les caractères. Nous pouvons donc commencer à déterminer la décomposition de $\chi_{\mathbb{C}[E]}$ comme combinaison linéaire de caractères irréductibles.

Déterminons $\left\langle \chi_{\mathbb{C}[E]}, \chi_0 \right\rangle$.

$$\begin{aligned}
\left\langle \chi_{\mathbb{C}[E]}, \chi_0 \right\rangle &= \frac{1}{168} \sum_{g \in G} \chi_{\mathbb{C}[E]}(g) \overline{\chi_0} \left(g^{-1}\right) \\
&= \frac{1}{168} \left(1 \cdot 21 \cdot 1 + 21 \cdot 5 \cdot 1 + 56 \cdot 0 \cdot 1 + 42 \cdot 1 \cdot 1 + 24 \cdot 0 \cdot 1 + 24 \cdot 0 \cdot 1\right) \\
&= \frac{21 + 105 + 42}{168} = \frac{168}{168} = 1
\end{aligned}$$

Ainsi nous ne trouvons la représentation triviale qu'une seule fois dans $\mathbb{C}[E]$.

Calculons $\left\langle \chi_{\mathbb{C}[E]}, \chi_6 \right\rangle$.

$$\begin{aligned}
\left\langle \chi_{\mathbb{C}[E]}, \chi_6 \right\rangle &= \frac{1}{168} \sum_{g \in G} \chi_{\mathbb{C}[E]}(g) \overline{\chi_6} \left(g^{-1}\right) \\
&= \frac{1}{168} \left(1 \cdot 21 \cdot 6 + 21 \cdot 5 \cdot 2 + 56 \cdot 0 \cdot 0 + 42 \cdot 1 \cdot 0 + 24 \cdot 0 \cdot (-1) + 24 \cdot 0 \cdot (-1)\right) \\
&= \frac{126 + 210}{168} = \frac{336}{168} = 2
\end{aligned}$$

Nous trouvons donc deux copies de la représentation de degré 6 dans $\mathbb{C}[E]$.

Posons $f \overset{\text{def}}{=} \chi_{\mathbb{C}[E]} - \chi_0 - 2\chi_6$.
Calculons $\langle f, f \rangle$:

$$\begin{aligned}
\langle f, f \rangle &= \frac{1}{168} \sum_{g \in G} f(g) \overline{f} \left(g^{-1}\right) \\
&= \frac{1}{168} \left(1(21 - 1 - 2 \cdot 6)^2 + 21(5 - 1 - 2 \cdot 2) + 56(0 - 1 - 2 \cdot 0)^2 + 42(1 - 1 - 2 \cdot 0)^2 + 48(0 - 1 - 2 \cdot (-1))^2\right) \\
&= \frac{64 + 56 + 48}{168} = \frac{168}{168} = 1
\end{aligned}$$

Ainsi f est un caractère irréductible, de degré $21 - 1 - 2 \cdot 6 = 8$ que nous noterons χ_8, dont les caractères sont :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_8	8	0	-1	0	1	1

3.3 Représentations de degré 3

Nous avons explicité quatre caractères du groupe simple d'ordre 168 : la représentation triviale, et les représentations de degré 6, 7 et 8 dont nous avons calculé les caractères.

De plus, nous savons que G admet autant de caractères irréductibles que de classes de conjugaisons, c'est-à-dire 6. Il nous manque donc deux représentations irréductibles, dont nous noterons n et m les degrés.

D'un autre côté, la somme des carrés des degrés des représentations irréductibles doit être égale à l'ordre du groupe, ici 168. Ainsi, nous avons :

$$168 = n^2 + m^2 + 1^2 + 6^2 + 7^2 + 8^2 \quad \text{c'est-à-dire} \quad n^2 + m^2 = 18$$

Nous savons également que le degré d'une représentation irréductible de G divise son ordre, ainsi n et m sont des diviseurs de 168 qui ne peuvent dépasser $\left\lfloor \sqrt{18} \right\rfloor = 4$, et donc $n, m \in [\![1, 4]\!]$.

- Si $n = 1$ alors $m^2 = 17$ ce qui est impossible puisque m est entier.
- Si $n = 2$ alors $m^2 = 14$, qui est aussi impossible.
- Si $n = 3$ alors $m^2 = 9$, donc $m = 3$ fonctionne.
- Si $n = 4$ alors $m^2 = 2$ ce qui est aussi impossible.

Finalement $n = m = 3$, et les deux représentations irréductibles manquantes sont de degré 3.

3.3.1 Anneau des entiers algébriques

Avant de se lancer dans le calcul des caractères des deux représentations de degré 3, nous faisons une petite digression qui nous sera utile.

Définition 3.3.1 (Entier algébrique)**.** *On appelle* entier algébrique (de $\mathbb{C}$) *toute racine d'un polynôme unitaire à coefficient dans $\mathbb{Z}$. Nous noterons $\mathcal{O}_{\mathbb{C}}$ l'ensemble des entiers algébriques (de $\mathbb{C}$).*

Proposition 3.3.2. *L'ensemble des entiers algébriques $\mathcal{O}_{\mathbb{C}}$ est un sous-anneau de $\mathbb{C}$.*

Démonstration. Il est clair que $1 \in \mathcal{O}_{\mathbb{C}}$ puisque 1 est racine du polynôme unitaire $X - 1 \in \mathbb{Z}[X]$, et en particulier $\mathcal{O}_{\mathbb{C}}$ est non-vide.
Prenons donc $\alpha \in \mathcal{O}_{\mathbb{C}}$. Il existe alors $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$, dont on note n le degré.
On a alors que $-\alpha$ est racine du polynôme $(-1)^{\deg P} P(-X) \in \mathbb{Z}[X]$ également unitaire, donc $-\alpha \in \mathcal{O}_{\mathbb{C}}$.

Choisissons $\beta \in \mathcal{O}_{\mathbb{C}}$, annulé par $Q \in \mathbb{Z}[X]$ unitaire, dont nous noterons m le degré.
On veut montrer que $\alpha + \beta \in \mathcal{O}_{\mathbb{C}}$. Pour cela, notons $\alpha_1 = \alpha$ et $\beta_1 = \beta$, et posons $(\alpha_i)_{i\in[\![1,n]\!]}$, $(\beta_j)_{j\in[\![1,m]\!]}$ les racines respectives de P et de Q dans $\mathbb{C}$.
Posons $R = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i - \beta_j)$. C'est bien un polynôme unitaire qui annule α et β, il nous faut maintenant montrer que c'est un polynôme à coefficients dans $\mathbb{Z}$. On remarque que :

$$R = \prod_{i=1}^{n} \prod_{j=1}^{m} \big((X - \alpha_i) - \beta_j\big) = \prod_{i=1}^{n} Q(X - \alpha_i)$$

Considérons $S(X, X_1, \cdots, X_n) = \prod_{i=1}^{n} Q(X - X_i)$. C'est un polynôme symétrique en les $(X_i)_{i\in[\![1,n]\!]}$, ainsi par le théorème fondamental des polynômes symétriques, le polynôme S est donc dans $A[\Sigma_1, \cdots, \Sigma_n]$ avec $A = \mathbb{Z}[X]$, où les $(\Sigma_i)_{i\in[\![1,n]\!]}$ sont les polynômes symétriques élémentaires. Il existe donc $T \in \mathbb{Z}[X][X_1, \cdots, X_n]$ tel que :

$$S(X, X_1 \cdots, X_n) = T(X, \Sigma_1, \cdots, \Sigma_n)$$

On a alors $R = T(X, \Sigma_1(\alpha_1, \cdots, \alpha_n), \cdots, \Sigma_n(\alpha_1, \cdots, \alpha_n))$. Or, par les relations coefficients-racines, pour tout $i \in [\![1, n]\!]$, $\Sigma_i(\alpha_1, \cdots, \alpha_n)$ est le coefficient en X^i de P, et donc est dans $\mathbb{Z}$, et donc R est bien un polynôme à coefficients dans $\mathbb{Z}$.
Donc $\alpha + \beta \in \mathcal{O}_{\mathbb{C}}$.

Pour le produit, on procède avec un raisonnement analogue, en considérant $R = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i \beta_j)$, unitaire et annulateur de $\alpha\beta$. On remarque que :

$$R = \prod_{i=1}^{n} \prod_{j=1}^{m} \left(\alpha_i \left(\frac{X}{\alpha_i} - \beta_j\right)\right) = \prod_{i=1}^{n} a_i^m Q\left(\frac{X}{\alpha_i}\right)$$

En posant $S(X, X_1, \cdots, X_n) = \prod_{i=1}^{n} X_i^m Q\left(\frac{X}{X_i}\right)$, symétrique en les $(X_i)_{i\in[\![1,n]\!]}$, on exhibe $T \in \mathbb{Z}[X][X_1, \cdots, X_n]$ tel que :

$$S(X, X_1 \cdots, X_n) = T(X, \Sigma_1, \cdots, \Sigma_n)$$

Pour les mêmes raisons, $R = T(X, \Sigma_1(\alpha_1, \cdots, \alpha_n), \cdots, \Sigma_n(\alpha_1, \cdots, \alpha_n))$ est un polynôme à coefficients entiers, et finalement $\alpha\beta \in \mathcal{O}_{\mathbb{C}}$.

Ainsi, $\mathcal{O}_{\mathbb{C}}$ est un anneau. □

Corollaire 3.3.3. *Les caractères d'un groupe fini sont des entiers algébriques.*

Démonstration. Soit G un groupe fini, et (V, ρ) une représentation de G, et soit $g \in G$, d'ordre n.
Le caractère $\chi_V(g)$ est la trace de l'endomorphisme $\rho(g)$, dont on sait qu'il vérifie $\rho(g)^n = \rho(g^n) = \rho\left(1_G\right) = \mathrm{id}_V$. Ainsi le polynôme $X^n - 1$ annule $\rho(g)$, donc son polynôme caractéristique divise $X^n - 1$. En particulier les racines de ce polynôme caractéristique sont des racines n-ièmes de l'unité, donc $\chi_V(g) = \mathrm{tr}\,\rho(g)$ est une somme finie de racines de l'unité.
On remarque que les racines n-ièmes de l'unité sont des entiers algébriques puisqu'elles sont annulées par le polynôme $X^n - 1$ unitaire à coefficients dans $\mathbb{Z}$. L'ensemble des entiers algébriques étant un anneau, $\chi_V(g) \in \mathcal{O}_{\mathbb{C}}$. □

Proposition 3.3.4. *Les entiers algébriques rationnels sont entiers. Autrement dit, $\mathcal{O}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$.*

Démonstration. Nous pouvons raisonner avec des rationnels sous forme irréductible. Considérons le rationnel p/q avec p, q premiers entre eux : si ce rationnel est racine d'un polynôme $P \in \mathbb{Z}[X]$ unitaire avec $P = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$, alors :

$$a_0 q^n + a_1 p q^{n-1} + \cdots + a_{n-1} p^{n-1} q + p^n = 0 \qquad \text{donc} \qquad q\left(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-1}\right) = -p^n$$

Puisque p et q sont premiers entre eux, q divise -1, donc $q = \pm 1$, et le rationnel p/q est alors entier. Réciproquement, il est clair que $\mathbb{Z}$ est dans $\mathcal{O}_{\mathbb{C}} \cap \mathbb{Q}$ puisque tout $n \in \mathbb{Z}$ est annulé par $X - n \in \mathbb{Z}[X]$ unitaire. □

3.3.2 Calcul des caractères

Nous savons qu'il y a deux représentations irréductibles de degré 3, dont nous noterons $\chi_3^{(1)}$ et $\chi_3^{(2)}$ les caractères respectifs. Nous voulons calculer ces caractères en utilisant les autres représentations irréductibles et les propriétés des tables de caractères. Écrivons :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_0	1	1	1	1	1	1
$\chi_3^{(1)}$	3	a	b	c	d	e
$\chi_3^{(2)}$	3	f	g	h	k	ℓ
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

où $a, b, c, d, e, f, g, h, k$ et ℓ sont des nombres complexes (évitons d'utiliser les lettres i et j pour éviter de les confondre avec des racines de $X^2 + 1$ ou $X^2 + X + 1$).

Deux colonnes distinctes sont « orthogonales », donc en prenant le produit hermitien entre la première colonne et les autres, nous parviendrons à déterminer des relations entre certains coefficients.

- Le produit hermitien de la deuxième colonne avec la deuxième donne :

$$1 \cdot 1 + 3\overline{a} + 3\overline{f} + 6 \cdot 2 + 7 \cdot (-1) + 8 \cdot 0 = 0 \quad \text{ie} \quad a + f = -2$$

- Avec la troisième colonne :

$$1 \cdot 1 + 3\overline{b} + 3\overline{g} + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot (-1) = 0 \quad \text{ie} \quad b + g = 0$$

- Pour la quatrième :

$$1 \cdot 1 + 3\overline{c} + 3\overline{h} + 6 \cdot 0 + 7 \cdot (-1) + 8 \cdot 0 = 0 \quad \text{ie} \quad c + h = 2$$

- Cinquième et sixième colonnes :

$$1\cdot 1+3\overline{d}+3\overline{k}+6\cdot(-1)+7\cdot 0+8\cdot 1=0 \quad \text{ie} \quad d+k=-1$$
$$1\cdot 1+3\overline{e}+3\overline{\ell}+6\cdot(-1)+7\cdot 0+8\cdot 1=0 \quad \text{ie} \quad e+\ell=-1$$

Réécrivons notre table en utilisant ces informations :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_0	1	1	1	1	1	1
$\chi_3^{(1)}$	3	a	b	c	d	e
$\chi_3^{(2)}$	3	$-2-a$	$-b$	$2-c$	$-1-d$	$-1-e$
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

Maintenant, et à l'aide de certaines relations entre coefficient calculées à l'aide des produits hermitiens, déterminons certains caractères.

Nous effectuons tout d'abord le produit hermitien entre les deux dernières colonnes, ce qui nous donne :

$$1\cdot 1+d\cdot\overline{e}+(1+d)(1+\overline{e})-1\cdot(-1)+0\cdot 0+1\cdot 1=0 \quad \text{ie} \quad 2d\overline{e}+d+\overline{e}+4=0 \qquad (\heartsuit)$$

À l'aide de cette relation, nous allons pouvoir déterminer quelques caractères.

- Effectuons les produits hermitiens entre la deuxième et la cinquième colonne, et la deuxième et la sixième colonne :

$$1\cdot 1+a\overline{d}+(2+a)(1+\overline{d})+2\cdot(-1)-1\cdot 0+0\cdot 1=0 \quad \text{ie} \quad (a+1)(2\overline{d}+1)=0$$
$$1\cdot 1+a\overline{e}+(2+a)(1+\overline{e})+2\cdot(-1)-1\cdot 0+0\cdot 1=0 \quad \text{ie} \quad (a+1)(2\overline{e}+1)=0$$

  Supposons que $a\neq -1$. Alors nécessairement, $\overline{d}=\overline{e}=\dfrac{1}{2}$ par ces deux relations, et donc $d=\dfrac{1}{2}$.
  Mais on remarque que :

$$2d\overline{e}+d+\overline{e}+4=\frac{2}{4}+\frac{1}{2}+\frac{1}{2}+4=\frac{11}{2}$$

  Les valeurs de d et e sont donc incompatibles avec l'égalité ($\heartsuit$), ainsi $a=-1$.

- Cette fois-ci, effectuons les produits entre la troisième et la cinquième colonne, et la troisième et sixième colonne :

$$1\cdot 1+b\overline{d}+b(1+\overline{d})+0\cdot(-1)+1\cdot 0-1\cdot 1=0 \quad \text{ie} \quad b(1+2\overline{d})=0$$
$$1\cdot 1+b\overline{e}+b(1+\overline{e})+0\cdot(-1)+1\cdot 0-1\cdot 1=0 \quad \text{ie} \quad b(1+2\overline{e})=0$$

  Supposons alors que $b\neq 0$. Alors $\overline{d}=\overline{e}=\dfrac{1}{2}$, ce qui contredit ($\heartsuit$). On en déduit que $b=0$.

- Une dernière fois entre la quatrième et les deux dernières colonnes :

$$1\cdot 1+c\overline{d}-(2-c)(1+\overline{d})+0\cdot(-1)-1\cdot 0+0\cdot 1=0 \quad \text{ie} \quad (c-1)(2\overline{d}+1)=0$$
$$1\cdot 1+c\overline{e}-(2-c)(1+\overline{e})+0\cdot(-1)-1\cdot 0+0\cdot 1=0 \quad \text{ie} \quad (c-1)(2\overline{e}+1)=0$$

  De la même manière, si $c\neq 1$, alors $\overline{d}=\overline{e}=\dfrac{1}{2}$, ce qui est impossible sans contredire l'orthogonalité des dernières colonnes donnée par ($\heartsuit$). Ainsi $c=1$.

De plus, nous savons que deux lignes distinctes sont « orthogonales » (le produit hermitien est pondéré par les ordres de chaque classe), ce qui donne, en effectuant ce produit hermitien entre les caractère $\chi_3^{(1)}$ et χ_8 :

$$1\cdot 3\cdot 8+21\cdot a\cdot 0+56\cdot b\cdot(-1)+42\cdot c\cdot 0+24d+24e=0$$

Avec les valeurs nouvellement déterminées de a, b et c, nous avons :

$$24+24d+24e=0 \qquad \text{ie} \qquad d+e=-1$$

Nous pouvons donc compléter un peu plus notre table des caractères grâce aux valeurs de a, b et c calculées et la nouvelle relation $e = -1 - d$, ce qui nous donne :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_0	1	1	1	1	1	1
$\chi_3^{(1)}$	3	-1	0	1	d	$-1-d$
$\chi_3^{(2)}$	3	-1	0	1	$-1-d$	d
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

Les quatre valeurs restantes résistent à des calculs similaires, il va donc falloir chercher plus loin.

Supposons que les caractères de la première représentation irréductible de degré 3 soient tous réels. Le produit scalaire entre les deux dernières colonnes déterminé à (♥) devient alors :

$$2d(-1-d) + d + (-1-d) + 4 = 0 \qquad \text{ie} \qquad d^2 + d - \frac{3}{2} = 0$$

Rappelons que d est un caractère d'une représentation de G, ainsi par le *corollaire 3.3.3*, d doit alors être un entier algébrique. Puisque $\mathcal{O}_{\mathbb{C}}$ est un anneau, $d^2 + d \in \mathcal{O}_{\mathbb{C}}$, c'est-à-dire que $\frac{3}{2} \in \mathcal{O}_{\mathbb{C}}$, ce qui est impossible d'après la *proposition 3.3.4* : $\mathcal{O}_{\mathbb{C}}$ ne contient en effet pas d'autres rationnels que les entiers.
Ainsi $d \notin \mathbb{R}$.

La première des deux représentations irréductibles de degré 3 n'est ainsi pas réelle, et est donc distincte de sa représentation conjuguée, qui est alors une autre représentation irréductible de degré 3. Puisque G n'admet que deux représentations irréductibles de degré 3, nous n'avons pas le choix :

$$\chi_3^{(1)} = \overline{\chi_3^{(2)}}$$

Cela nous permet donc de dire que $\overline{d} = -1 - d$. Puisque $\chi_3^{(1)}$ est irréductible, nous avons que son produit hermitien avec elle-même vaut 1, donc :

$$9 + 21 + 42 + 24d\overline{d} + 24d\overline{d} = 168 \qquad \text{ie} \qquad d\overline{d} = 2$$

Ces informations nous donnent que d est racine du polynôme $(X-d)(X-\overline{d}) = X^2 - (d+\overline{d})X + d\overline{d} = X^2 + X + 2$. Ce polynôme admet pour racines $\frac{-1 \pm i\sqrt{7}}{2}$. Quitte à intervertir $\chi_3^{(1)}$ et $\chi_3^{(2)}$, nous prenons $d = \frac{-1+i\sqrt{7}}{2}$.

Finalement, pour les deux représentations irréductibles de degré 3, nous avons les caractères suivants :

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
$\chi_3^{(1)}$	3	-1	0	1	$\frac{-1+i\sqrt{7}}{2}$	$\frac{-1-i\sqrt{7}}{2}$
$\chi_3^{(2)}$	3	-1	0	1	$\frac{-1-i\sqrt{7}}{2}$	$\frac{-1+i\sqrt{7}}{2}$

3.4 Table des caractères

En regroupant toutes les informations des parties précédentes, nous avons :

Propriété. *La table des caractères du groupe simple d'ordre* 168 *est la table suivante :*

Ordre	1	2	3	4	7	7
Cardinal	1	21	56	42	24	24
χ_0	1	1	1	1	1	1
$\chi_3^{(1)}$	3	-1	0	1	α	$\overline{\alpha}$
$\chi_3^{(2)}$	3	-1	0	1	$\overline{\alpha}$	α
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

où $\alpha = \frac{-1+i\sqrt{7}}{2}$.

Références

[1] Grégory Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[2] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries*. Calvage & Mounet, 2018.

[3] Ezra Brown et Nicholas Loehr. Why is psl (2,7) ≃ gl (3,2) ? *The American Mathematical Monthly*, 116(8) : 727–732, 2009.

[4] Ortiz Pascal. *Exercices d'algèbre*. Ellipses Paris, 2004.

[5] Daniel Perrin. *Cours d'algèbre*, volume 30. Ellipses Paris, 1996.

[6] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics 148. Springer-Verlag New York, 4 edition, 1995.

[7] Timothy Vis. The existence and uniqueness of a simple group of order 168. *Voir* `http://math.ucdenver.edu/~tvis/Coursework/Fano.pdf`, 2007.