ÉCOLE POLYTECHNIQUE.

ENSEIGNEMENT D'APPROFONDISSEMENT :

Groupes finis, représentations et caractères : théorèmes de Frobenius, de Burnside et de Suzuki.

Emmanuel Pinglier et Pierrick Dartois.

Abstract : Ce mémoire de M1 introduit les représentations linéaires des groupes finis. Nous l'appliquerons à trois résultats majeurs de théorie des groupes dont les preuves utilisent aussi des énoncés d'arithmétique, d'algèbre élémentaire et de théorie algébrique des nombres.

Nous démontrerons dans un premier temps le théorème de Frobenius. En substance, ce théorème assure que tout groupe *de Frobenius* (notion qui sera définie ultérieurement) s'écrit comme produit semi-direct.

Nous prouverons ensuite le célèbre théorème de Burnside (1902), selon lequel tout groupe dont l'ordre admet au plus deux facteurs premiers est résoluble.

Enfin, nous étudierons la preuve d'un autre résultat de résolubilité dû à Suzuki, démontré en 1957 et qui donne une première étape de la classification des groupes finis. Ce théorème de Suzuki est un cas particulier du théorème de Feit-Thompson (1962) selon lequel tout groupe fini d'ordre impair est résoluble. Suzuki a en fait prouvé cet énoncé pour les groupes *commutants abéliens* d'ordre impair. Les caractères que nous introduirons dans le cadre de la théorie des représentations linéaires des groupes finis sont un outil essentiel de cette preuve.

Table des matières

1 Représentations linéaries des groupes finis.

1.1 Définition et premiers exemples.

Il est souvent utile de faire agir des groupes sur des ensembles pour mieux en comprendre la structure. C'est notre objectif ici, une représentation linéaire n'étant rien d'autre qu'une action linéaire de groupe sur un espace vectoriel.

Définition 1.1.1. *Si G est un groupe, une* représentation linéaire *de G est la donnée d'un espace vectoriel V (sur un certain corps K) et d'une action à gauche de G sur V i.e. d'une application :*

$$\begin{array}{rcl} \bullet : G \times V & \longrightarrow & V \\ (g, x) & \longmapsto & g \bullet x \end{array}$$

telle que $e \bullet x = x$ et $g \bullet (h \bullet x) = (gh) \bullet x$ pour tous $x \in V$ et $g, h \in G$; l'action $\bullet$ ayant en outre une propriété de linéarité, c'est à dire que pour tout $g \in G$, $x \in V \longmapsto g \bullet x \in V$ est linéaire.

Remarque 1.1.2. Pour tout $g \in G$, $x \in V \longmapsto g \bullet x \in V$ est bijective d'inverse $x \in V \longmapsto g^{-1} \bullet x \in V$. De manière équivalente, on peut dire qu'une *représentation linéaire* de G est la donnée d'un morphisme de groupes $\rho_V : G \longrightarrow GL(V)$. C'est souvent ce point de vue qui sera adopté plus tard et on désignera toujours une représentation linéaire de G par le couple (V, ρ_V).

De même que pour les actions de groupes, on dira que la représentation est *fidèle* lorsque ρ_V est injective.

Exemple 1.1.3. Pour $G = \mathbb{Z}$ et (V, ρ_V) une représentation linéaire de $\mathbb{Z}$, $\rho_V(\mathbb{Z})$ est le sous-groupe de $GL(V)$ engendré par $u := \rho_V(1)$ car $\mathbb{Z}$ est engendré par 1. Donc une représentation (V, ρ_V) de $\mathbb{Z}$ est la donnée de V et d'un élément $u \in GL(V)$.

Exemple 1.1.4. Lorsque G est cyclique d'ordre n engendré par g et que (V, ρ_V) une représentation linéaire de G, $\rho_V(G)$ est cyclique d'ordre divisant n engendré par $u := \rho_V(g)$ vérifiant $u^n = \mathrm{id}_V$. Donc une représentation (V, ρ_V) de G est la donnée de V et d'un élément $u \in GL(V)$ d'ordre divisant n.

Exemple 1.1.5. Le premier exemple intéressant concerne le groupe non-abélien $\mathfrak{S}_3$. Il est aisé de voir que les permutations $\sigma_1 := (1, 2)$ et $\sigma_2 := (2, 3)$ engendrent $\mathfrak{S}_3$. On a par ailleurs $\sigma_1^2 = \sigma_2^2 = 1$ et $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ et toute autre relation dans $\mathfrak{S}_3$ peut s'écrire à partir de ces trois relations. Donc une représentation linéaire (V, ρ_V) de $\mathfrak{S}_3$ est entièrement déterminée par la donnée de l'espace V et de deux symétries [1] $s_1 := \rho_V(\sigma_1)$ et $s_2 := \rho_V(\sigma_2)$ telles que $s_1 s_2 s_1 = s_2 s_1 s_2$.

Un exemple classique de représentation linéaire fidèle de $\mathfrak{S}_3$ est le cas où $V = \mathbb{R}^2$ et où ρ_V stabilise le triangle équilatéral ABC centré en $O := (0, 0)$ avec $A := (1, 0)$, $B := \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ et $C := \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$. $\rho_V(\mathfrak{S}_3)$ préserve alors les normes de deux vecteurs linéairement indépendants, de sorte que $\rho_V(\mathfrak{S}_3) \subset O_2(\mathbb{R})$. En écrivant tous les éléments possibles de ce groupe dans la base canonique de $\mathbb{R}^2$, on voit qu'il ne peut y avoir que l'identité, les rotations d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$ et les symétries d'axe (OA), (OB) et (OC). Comme $|\mathfrak{S}_3| = 6$ et que la représentation est fidèle, $\rho_V(\mathfrak{S}_3)$ contient tous ces éléments. C'est en fait exactement le groupe diédral D_3. Cette représentation est un isomorphisme naturel entre $\mathfrak{S}_3$ et D_3 qui agit par permutation sur les sommets A, B et C du triangle.

On voit à travers ces exemples que l'on peut déterminer une représentation si l'on connait le groupe de départ. Notre objectif ici est de voir si la réciproque est possible. Peut-on bien connaître un groupe à partir de ses représentations linéaires ? Pour cela, la théorie des caractères que nous verrons au paragraphe suivant constitue un outil indispensable. Avant cela, terminons cette série d'exemples.

1. Par définition, une symétrie est une involution linéaire de V dans lui-même.

Exemple 1.1.6 (Représentation régulière)**.** Soient G un groupe fini et V un K-espace vectoriel de dimension $|G|$. Alors V admet une K-base indexée par G, notée $(e_g)_{g\in G}$. On appelle *représentation régulière* la représentation linéaire de G dans V donnée par :

$$\forall g, h \in G, \quad \rho(g)(e_h) = e_{gh}$$

Pour tout $g \in G$, $\rho(g)$ a pour matrice dans $(e_g)_{g\in G}$: $(\delta_{gh,k})_{h,k\in G}$, la matrice de permutation associée à $h \in G \longmapsto gh \in G$. La représentation régulière est en fait une permutation des vecteurs de bases.

Exemple 1.1.7 (Représentation canonique de $\mathfrak{S}_n$)**.** Si $(e_1, \cdots, e_n)$ est la base canonique de $\mathbb{C}^n$, on obtient une représentation linéaire de $\mathfrak{S}_n$ dans $\mathbb{C}^n$ en posant pour tous $\sigma \in \mathfrak{S}_n$ et $i \in \{1, \cdots, n\}$:

$$\rho(\sigma)(e_i) := e_{\sigma(i)}$$

Dans toute la suite de ce document, le groupe G considéré sera fini, le corps de base K de la représentation (V, ρ_V) sera le corps des nombres complexes $\mathbb{C}$ et V sera de dimension finie. Ceci donne un sens à la définition suivante.

Définition 1.1.8. *Sous les hypothèses ci-dessus, on appelle* degré *d'une représentation linéaire (ρ_V, V) la quantité $dim_{\mathbb{C}}(V)$.*

1.2 Irréductibilité, sous-représentation.

Définition 1.2.1. *Une représentation linéaire (V, ρ) d'un groupe fini G est dite* irréductible *lorsque les seuls sous-espaces vectoriels de V stables par l'action de G (i.e. les sous-espaces vectoriels $W \subset V$ tels que $\rho(g)(W) \subset W$ pour tout $g \in G$) sont $\{0\}$ et V.*

Sur un sous-espace vectoriel $W \subset V$ stable par l'action de G, on peut définir une sous-représentation *$(W, \rho_{|W})$ de (V, ρ) donnée par :*

$$\forall g \in G, \quad \rho_{|W}(g) := \rho(g)^{|W}_{|W}$$

On dira que le sous-espace W est irréductible lorsque $(W, \rho_{|W})$ est irréductible.

Exemple 1.2.2. La représentation de $\mathfrak{S}_3$ dans $\mathbb{R}^2$ donnée à l'exemple 1.1.5 est irréductible. Rappelons de quoi il s'agit. Etant donné les points $A := (1, 0)$, $B := \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ et $C := \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$ identifiés respectivement à 1, 2 et 3, on associe à $\sigma \in \mathfrak{S}_3$ l'unique isométrie $\rho(\sigma)$ du plan qui agit sur $\{A, B, C\}$ de la même façon que σ agit sur $\{1, 2, 3\}$. Si par l'absurde cette représentation n'était pas irréductible, elle stabiliserait une droite vectorielle de $\mathbb{R}^2$. Mais aucune droite de $\mathbb{R}^2$ n'est stable par la rotation d'angle $\frac{2\pi}{3}$ (qui est exactement $\rho((1, 2, 3))$).

Exemple 1.2.3. La représentation canonique de $\mathfrak{S}_n$ dans $\mathbb{C}^n$ vue à l'exemple 1.1.7 donnée par :

$$\forall \sigma \in \mathfrak{S}_n, \quad \forall i \in \{1, \cdots, n\}, \quad \rho(\sigma)(e_i) := e_{\sigma(i)}$$

où $(e_i)_{1\leq i\leq n}$ est la base canonique de $\mathbb{C}^n$ n'est pas irréductible. En effet, $\mathbb{C}u$ où $e := \sum_{i=1}^n e_i$ est stable sous l'action de $\mathfrak{S}_n$ et il en est de même pour son supplémentaire orthogonal :

$$W := \left\{ (x_1, \cdots, x_n) \in \mathbb{C}^n; \sum_{i=1}^n x_i = 0 \right\}$$

En revanche, $(\mathbb{C}e, \rho_{|\mathbb{C}e})$ et $(W, \rho_{|W})$ sont des sous-représentations irréductibles de $(\mathbb{C}^n, \rho)$. C'est immédiat pour $\mathbb{C}e$. Vérifions-le dans le cas de W. Soit $F \subset W$ un sous-espace stable sous l'action de $\mathfrak{S}_n$ non réduit à $\{0\}$. Il s'agit de montrer que $F = W$. Comme $F \subset W$ n'est pas réduit à $\{0\}$, il contient un élément $x \neq 0$ admettant deux composantes distinctes x_i et x_j (pour $1 \leq i < j \leq n$). Sinon, on aurait

$0 = \sum_{i=1}^{n} x_i = nx_k$ pour tout $k \in \{1, \cdots, n\}$ et donc $x = 0$. Mais la transposition (i, j) échange x_i et x_j et laisse invariante toutes les autres composantes. Il s'ensuit que :

$$e_i - e_j = \frac{1}{x_j - x_i}(\rho((i,j))(x) - x) = (0, \cdots, 0, \overbrace{1}^{(i)}, 0, \cdots, 0, \overbrace{-1}^{(j)}, 0, \cdots, 0) \in F$$

En faisant agir $(k, i)(k + 1, j)$ pour tout $k \in \{1, \cdots, n - 1\}$, on obtient aussi que $e_k - e_{k+1} \in F$. Or, on peut vérifier que la famille $(e_k - e_{k+1})_{1 \leq k \leq n-1}$ est libre donc $\dim F \geq n - 1 = \dim W$ et $F = W$.

On a donc décomposé $\mathbb{C}^n$ en somme directe de sous-espaces irréductibles. Nous verrons que l'on peut en fait toujours le faire en dimension finie sur $\mathbb{C}$. La démarche exposée dans cet exemple est cruciale pour traiter le cas général : trouver un sous-espace irréductible et un supplémentaire stable de ce sous-espace, puis travailler dans ce sous-espace et conclure par récurrence sur la dimension.

Lemme 1.2.4. *Soit (ρ, V) une représentation linéaire du groupe fini G, de degré fini sur $\mathbb{C}$. Alors si W est stable sous l'action de G, il existe un supplémentaire de W qui l'est aussi.*

Démonstration. Soit $(.|.)$ un produit scalaire hermitien quelconque sur V (il en existe toujours, quitte à se donner une base de V). On définit un autre produit scalaire $\langle ., . \rangle$ sur V par :

$$\forall v, w \in V, \quad \langle v, w \rangle := \frac{1}{|G|} \sum_{g \in G} (\rho(g)(v) | \rho(g)(w))$$

Cette "moyenne" du produit scalaire $(.|.)$ sur G a pour propriété d'être invariante sous l'action de G. En effet, si $g \in G$ et $v, w \in V$ alors :

$$\langle \rho(g)(v), \rho(g)(w) \rangle = \frac{1}{|G|} \sum_{h \in G} (\rho(h)(\rho(g)(v)) | \rho(h)(\rho(g)(w))) = \frac{1}{|G|} \sum_{h \in G} (\rho(hg)(v) | \rho(hg)(w))$$

Or, $h \in G \longmapsto hg \in G$ est une bijection de réciproque $h \in G \longmapsto hg^{-1} \in G$ donc par changement d'indice $k := hg$:

$$\langle \rho(g)(v), \rho(g)(w) \rangle = \frac{1}{|G|} \sum_{k \in G} (\rho(k)(v) | \rho(k)(v)) = \langle v, w \rangle$$

Soit S l'orthogonal de W pour ce produit scalaire $\langle ., . \rangle$. Alors si $v \in S$, on a pour tous $g \in G$ et $w \in W$, $\rho(g^{-1})w \in W$ et donc :

$$\langle \rho(g)(v), w \rangle = \langle \rho(g)(v), \rho(g)(\rho(g^{-1})w) \rangle = \langle v, \rho(g^{-1})w \rangle = 0$$

ce qui montre que S est stable sous l'action de G. □

Théorème 1.2.5 (Maschke)**.** *Soit (V, ρ) une représentation linéaire complexe de degré fini du groupe fini G. Alors V est somme directe de sous-espaces vectoriels irréductibles.*

Démonstration. C'est une récurrence sur la dimension de V utilisant le lemme précédent. □

Remarque 1.2.6. Une preuve alternative, valable sur tout corps de caractéristique ne divisant pas $|G|$ utilise l'endomorphisme moyenne $p := \frac{1}{|G|} \sum_{g \in G} \rho(g)$. On peut montrer que c'est un projecteur dont le noyau et l'image (qui sont en somme directe) sont stables par G.

1.3 Caractères.

Définition 1.3.1. *Si G est un groupe fini et si (V,ρ) est une représentation linéaire complexe finie dimensionnelle de G*[2]*, alors on appelle* caractère *associé à la représentation (V,ρ) et on note χ_ρ l'application :*

$$\begin{array}{rccc} \chi_\rho : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & Tr(\rho(g)) \end{array}$$

Le caractère χ_ρ est dit irréductible *lorsque (V,ρ) est irréductible.*

Exemple 1.3.2 (Caractère de la représentation régulière)**.** On se place dans le cas de l'exemple 1.1.6. V est un $\mathbb{C}$-espace vectoriel complexe de dimension $|G|$ muni d'une base $(e_g)_{g\in G}$ (par exemple $\mathbb{C}^G$ muni de $(\delta_g)_{g\in G}$) et ρ_0 est la représentation linéaire de G définie par :

$$\forall g,h\in G,\quad \rho(g)(e_h) := e_{gh}$$

Dans $(e_h)_{h\in G}$, $\rho(g)$ a pour matrice $(\delta_{k,gh})_{(k,h)\in G^2}$ pour tout $g\in G$. Les coefficients diagonaux non nuls de cette matrice sont tels que $gh=h$. Il y en a donc soit aucun soit $|G|$ tous égaux à 1 (dans le cas où $g=1$ seulement). Ainsi :

$$\forall g\in G,\quad \chi_\rho(g) = \mathrm{Tr}(\rho(g)) = |G|\delta_{g,1}$$

Avant d'énoncer les propriétés des caractères, il est essentiel de faire le constat suivant :

Remarque 1.3.3. Comme G est fini, le théorème de Lagrange assure que pour tout $g\in G$, $g^{|G|}=e$, de sorte que $\rho(g)^{|G|} = \mathrm{id}_V$. Donc $X^{|G|}-1$ est un polynôme annulateur de $\rho(g)$ et comme ce polynôme est scindé à racines simples dans $\mathbb{C}$ (qui sont exactement les racines $|G|$-ièmes de l'unité), $\rho(g)$ est diagonalisable et ses valeurs propres sont des racines $|G|$-ièmes de l'unité.

Proposition 1.3.4. *Les caractères vérifient les propriétés suivantes :*

- **(i)** $\chi_\rho(1) = dim(V)$.
- **(ii)** $\forall g,h\in G,\quad \chi_\rho(ghg^{-1}) = \chi_\rho(h)$. *Autrement dit, χ_ρ est constante sur les classes de conjugaison de G. On dira que χ_ρ est* une fonction centrale.
- **(iv)** *L'ensemble $ker\chi_\rho := \{g\in G | \chi_\rho(g) = \chi_\rho(1)\}$ appelé* noyau *de χ_ρ est égale au noyau de ρ. C'est en particulier un sous-groupe distingué de G.*

Démonstration. On a $\rho(1)=\mathrm{id}_V$ qui est de trace $\dim(V)$. Le premier point est alors immédiat.

Comme $\mathrm{Tr}(u\circ v) = \mathrm{Tr}(v\circ u)$ pour tous $u,v\in L(V)$, on a pour tous $g,h\in G$:

$$\chi_\rho(ghg^{-1}) = \mathrm{Tr}(\rho(ghg^{-1})) = \mathrm{Tr}(\rho(g)\rho(h)\rho(g)^{-1}) = \mathrm{Tr}(\rho(g)^{-1}\rho(g)\rho(h)) = \mathrm{Tr}(\rho(g)) = \chi_\rho(h)$$

Enfin, si $g\in G$ et si on note $\lambda_1,\cdots,\lambda_n$ les valeurs propres de $\rho(g)$ comptées avec multiplicitées alors :

$$\chi_\rho(g) = \sum_{i=1}^{n}\lambda_i$$

Et comme les λ_i sont des racines de l'unité (d'après la remarque 1.3.3), on a pour tout $i\in\{1,\cdots,n\}$, $\lambda_i^{-1} = \overline{\lambda_i}$. Or, les valeurs propres de $\rho(g^{-1}) = \rho(g)^{-1}$, ne sont autres que $\lambda_1^{-1},\cdots,\lambda_n^{-1}$. Ainsi :

$$\chi_\rho(g^{-1}) = \sum_{i=1}^{n}\lambda_i^{-1} = \sum_{i=1}^{n}\overline{\lambda_i} = \overline{\sum_{i=1}^{n}\lambda_i} = \overline{\chi_\rho(g)}$$

2. Ces hypothèses, déjà énoncées à la fin du paragraphe précédent, ne seront pas reprécisées dans la suite.

Enfin, si $g \in \ker(\chi)$ alors :

$$\sum_{i=1}^{n} \lambda_i = \chi_\rho(g) = \chi_\rho(1) = \dim(V) = n$$

Donc il y a en particulier cas d'égalité dans l'inégalité triangulaire et tous les λ_i sont positivement liés, donc égaux car de module 1. Ainsi $n\lambda_1 = n$ et $\lambda_1 = 1$ donc tous les λ_i valent 1 et $\rho(g) = \mathrm{id}_V$ i.e. $g \in \ker(\rho)$. Réciproquement, tout élément de $\ker(\rho)$ est trivialement de caractère égal à $\dim(V) = \chi_\rho(1)$. D'où (iv). □

Nous allons voir maintenant comment se comportent les caractères sous l'effet d'opérations simples sur les représentations qui permettent de construire de nouveaux caractères à partir de caractères connus. Soient (V_1, ρ_1) et (V_2, ρ_2) des représentations linéaires (complexes et fini dimensionnelles) du groupe fini G.

Définition 1.3.5 (Somme directe de représentations)**.** *On désigne par $\rho_1 \oplus \rho_2$ la représentation linéaire de G définie sur $V_1 \times V_2$ par :*

$$\forall g \in G, \quad \forall (v_1, v_2) \in V_1 \times V_2, \quad \rho_1 \oplus \rho_2(g)(v_1, v_2) := (\rho_1(g)(v_1), \rho_2(g)(v_2))$$

Cette représentation linéaire est appelée somme directe *des représentations (ρ_1, V_1) et (ρ_2, V_2).*

Si $(V_1, \rho_1), \cdots, (V_r, \rho_r)$ sont des représentations linéaires de G et $m_1, \cdots, m_r \in \mathbb{N}$, on peut plus généralement définir par récurrence la représentation $(\prod_{i=1}^{r} V_i^{m_i}, \bigoplus_{i=1}^{r} m_i\rho_i)$, m_i étant le nombre de répétitions de la représentation (V_i, ρ_i) dans la somme directe.

Proposition 1.3.6.

$$\forall g \in G, \quad \chi_{\rho_1 \oplus \rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g)$$

Démonstration. Soient $\mathcal{B} := (e_1, \cdots, e_n)$ et $\mathcal{C} := (f_1, \cdots, f_m)$ des bases respectives de V_1 et V_2. Alors $\mathcal{D} := ((e_1, 0), \cdots, (e_n, 0), (0, f_1), \cdots, (0, f_m))$ est une base de $V_1 \times V_2$. Pour $g \in G$, notons $M_1(g)$ et $M_2(g)$ respectivement les matrices de $\rho_1(g)$ dans $\mathcal{B}$ et de $\rho_2(g)$ dans $\mathcal{C}$. Alors la matrice de $\rho_1 \oplus \rho_2(g)$ dans $\mathcal{D}$ est :

$$\begin{pmatrix} M_1(g) & 0 \\ 0 & M_2(g) \end{pmatrix}$$

de sorte que :

$$\chi_{\rho_1 \oplus \rho_2}(g) = \mathrm{Tr}(rho_1 \oplus \rho_2(g)) = \mathrm{Tr}(M_1(g)) + \mathrm{Tr}(M_2(g)) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g)$$

□

Pour ce qui suit, on pourra se reporter à l'annexe A.1 donnant introduisant la notion de produit tensoriel d'espaces vectoriels.

Définition 1.3.7 (Produit tensoriel de représentations)**.** *On désigne par $\rho_1 \otimes \rho_2$ la représentation linéaire de G définie sur $V_1 \otimes V_2$ par :*

$$\forall g \in G, \quad \rho_1 \otimes \rho_2(g) := \rho_1(g) \otimes \rho_2(g)$$

Cette représentation linéaire est appelée produit tensoriel *des représentations (ρ_1, V_1) et (ρ_2, V_2).*

Proposition 1.3.8.

$$\forall g \in G, \quad \chi_{\rho_1 \otimes \rho_2}(g) = \chi_{\rho_1}(g)\chi_{\rho_2}(g)$$

Démonstration. Soient $\mathcal{B} := (e_1, \cdots, e_n)$ et $\mathcal{C} := (f_1, \cdots, f_m)$ des bases respectives de V_1 et V_2. Alors $\mathcal{D} := (e_i f_j)_{\substack{1\leq i\leq n \\ 1\leq j\leq m}}$ est une base de $V_1 \otimes V_2$. Pour $g \in G$, notons $M_1(g)$ et $M_2(g)$ respectivement les matrices de $\rho_1(g)$ dans $\mathcal{B}$ et de $\rho_2(g)$ dans $\mathcal{C}$. Alors d'après la proposition A.1.5, la matrice de $\rho_1 \otimes \rho_2(g)$ dans $\mathcal{D}$ est :

$$M_1(g) \otimes M_2(g) = (M_1(g)_{i,j} M_2(g))_{1\leq i,j\leq n}$$

de sorte que :

$$\begin{aligned}\chi_{\rho_1\otimes\rho_2}(g) = \mathrm{Tr}(\rho_1 \otimes \rho_2(g)) = \mathrm{Tr}(M_1(g) \otimes M_2(g)) &= \sum_{i=1}^{n}\sum_{j=1}^{m} M_1(g)_{i,i} M_2(g)_{j,j} \\ = \left(\sum_{i=1}^{n} M_1(g)_{i,i}\right)\left(\sum_{j=1}^{m} M_2(g)_{j,j}\right) &= \mathrm{Tr}(M_1(g))\mathrm{Tr}(M_2(g)) = \chi_{\rho_1}(g)\chi_{\rho_2}(g)\end{aligned}$$

□

1.4 Morphisme de représentations.

Définition 1.4.1. *Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations linéaires du groupe fini G. Alors on définit $H(\rho_1, \rho_2) : G \longrightarrow L(V_1, V_2)$ par :*

$$\forall g \in G, \quad \forall u \in L(V_1, V_2), \quad H(\rho_1, \rho_2)(g)(u) := \rho_2(g) \circ u \circ \rho_1(g)^{-1}$$

C'est une représentation linéaire de G dans $L(V_1, V_2)$ appelé morphisme *entre (V_1, ρ_1) et (V_2, ρ_2).*

Vérifions que la définition précédente a un sens, c'est-à-dire que $H(\rho_1, \rho_2)$ est bien une représentation linéaire de G dans $L(V_1, V_2)$. Pour tout $g \in G$, $H(\rho_1, \rho_2)(g)$ est clairement linéaire de $L(V_1, V_2)$ dans lui-même et c'est un isomorphisme d'inverse $H(\rho_1, \rho_2)(g^{-1})$. Donc $H(\rho_1, \rho_2)$ est à valeurs dans $GL(L(V_1, V_2))$. En outre, si $g, h \in G$ et $u \in L(V_1, V_2)$ alors :

$$\begin{aligned}H(\rho_1, \rho_2)(g) \circ H(\rho_1, \rho_2)(h)(u) &= H(\rho_1, \rho_2)(g)(\rho_2(h) \circ u \circ \rho_1(h)^{-1}) \\ &= \rho_2(g) \circ \rho_2(h) \circ u \circ \rho_1(h)^{-1} \circ \rho_1(g)^{-1} \\ &= \rho_2(gh) \circ u \circ \rho_1(gh)^{-1} = H(\rho_1, \rho_2)(gg')(u)\end{aligned}$$

Ce qui montre bien que $H(\rho_1, \rho_2)$ est un morphisme de groupes de G vers $GL(L(V_1, V_2))$, donc une représentation linéaire de G dans $L(V_1, V_2)$.

Proposition 1.4.2. *Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations linéaires du groupe fini G. Alors :*

$$\forall g \in G, \quad \chi_{H(\rho_1,\rho_2)} = \overline{\chi_{\rho_1}(g)}\chi_{\rho_2}(g)$$

Démonstration. Soit $g \in G$. On a vu dans la remarque 1.3.3 que $\rho_1(g)$ et $\rho_2(g)$ sont diagonalisables et que leurs valeurs propres sont des racines de l'unité (puisque G est fini). On dispose donc de $\mathcal{B} := (e_i)_{1\leq i\leq n}$ et $\mathcal{C} := (f_j)_{1\leq j\leq m}$ bases respectives de V_1 et V_2 dans lesquelles les matrices de $\rho_1(g)$ et de $\rho_2(g)$ respectivement sont diagonales. On peut alors écrire :

$$\forall i \in \{1, \cdots, n\}, \quad \rho_1(g)(e_i) = \lambda_i e_i \quad \text{et} \quad \forall j \in \{1, \cdots, m\}, \quad \rho_2(g)(f_j) = \mu_j f_j$$

où les λ_i et les μ_j sont des racines de l'unité. Soit pour tout $(i, j) \in \{1, \cdots, n\} \times \{1, \cdots, m\}$, l'application linéaire $u_{i,j} \in L(V_1, V_2)$ donnée par :

$$\forall k \in \{1, \cdots, n\}, \quad u_{i,j}(e_k) = \delta_{i,k} f_j$$

Alors $(u_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq m}}$ est une base de $L(V_1,V_2)$ et pour tous $(i,j)\in\{1,\cdots,n\}\times\{1,\cdots,m\}$ et $k\in\{1,\cdots,n\}$:

$$H(\rho_1,\rho_2)(u_{i,j})(e_k)=\rho_2(g)\circ u_{i,j}\circ\rho_1(g)^{-1}(e_k)=\rho_2(g)\circ u_{i,j}(\lambda_k^{-1}e_k)=\rho_2(g)(\lambda_i^{-1}\delta_{i,k}f_j)=\lambda_i^{-1}\mu_j\delta_{i,k}f_j$$

Donc $H(\rho_1,\rho_2)(u_{i,j})=\lambda_i^{-1}\mu_j u_{i,j}=\overline{\lambda_i}\mu_j u_{i,j}$. Puis :

$$\begin{aligned}\chi_{H(\rho_1,\rho_2)}(g)&=\mathrm{Tr}(H(\rho_1,\rho_2)(g))=\sum_{i=1}^{n}\sum_{j=1}^{m}\overline{\lambda_i}\mu_j=\left(\overline{\sum_{i=1}^{n}\lambda_i}\right)\left(\sum_{j=1}^{m}\mu_j\right)=\overline{\mathrm{Tr}(\rho_1(g))}\mathrm{Tr}(\rho_2(g))\\&=\overline{\chi_{\rho_1}(g)}\chi_{\rho_2}(g)\end{aligned}$$

□

Définition 1.4.3. *On dit que deux représentations linéaires (V_1,ρ_1) et (V_2,ρ_2) d'un groupe G sont* isomorphes *lorsqu'il existe un isomorphisme linéaire $u\in GL(V_1,V_2)$ invariant sous l'action de G via la représentation $H(\rho_1,\rho_2)$ i.e. tel que :*

$$\forall g\in G,\quad H(\rho_1,\rho_2)(g)(u)=u\Longleftrightarrow u=\rho_2(g)\circ u\circ\rho_1(g)^{-1}\Longleftrightarrow\rho_2(g)=u\circ\rho_1(g)\circ u^{-1}$$

Remarque 1.4.4. On voit donc que deux représentations isomorphes ont même degré ($\dim V_1=\dim V_2$) et surtout même caractère. On verra (ce qui est beaucoup plus fort) que la réciproque de ce résultat est vraie.

1.5 Orthogonalité des caractères et applications.

Dans toute la suite, on fixe G un groupe fini. On notera $L^2(G)$ la $\mathbb{C}$-algèbre hermitienne des fonctions de G dans $\mathbb{C}$ muni du produit scalaire $\langle .,.\rangle$ donné par :

$$\forall f_1,f_2\in L^2(G),\quad\langle f_1,f_2\rangle=\frac{1}{|G|}\sum_{g\in G}f_1(g)\overline{f_2(g)}$$

Ce produit scalaire sera parfois noté $\langle .,.\rangle_G$ pour préciser la dépendance en G. Commençons par remarquer que $L^2(G)$ est de dimension finie de base $(\delta_g)_{g\in G}$ où pour tout $g\in G$, δ_g est le dirac en G.

On désignera par $L^2(G)^G$ la sous-$\mathbb{C}$-algèbre de $L^2(G)$ formée par les fonctions centrales :

$$L^2(G)^G:=\{f\in L^2(G)|\quad\forall g,h\in G,\quad f(ghg^{-1})=f(h)\}$$

elle contient en particulier les caractères.

On notera aussi $L^2(G)^G_{\mathbb{Z}}$, l'ensemble des *carctères généralisés* de G, c'est à dire la sous-$\mathbb{Z}$-algèbre de $L^2(G)^G$ engendrée par les caractères. Avec les propositions 1.3.6 et 1.3.8, on voit que toute combinaison linéaire entière à coefficients positifs de caractères est un caractère et que tout produit de caractère est un caractère. Il s'ensuit que tout élément de $L^2(G)^G_{\mathbb{Z}}$ s'écrit sous la forme $\epsilon\chi-\epsilon'\chi'$ où χ et χ' sont des caractères et $\epsilon,\epsilon'\in\{0,1\}$.

Enfin, on notera $\mathrm{Irr}(G)$ l'ensemble des caractères irréductibles de G. Le but de ce paragraphe est de montrer qu'en fait $\mathrm{Irr}(G)$ est une base orthonormée de $L^2(G)^G$ et de voir quelques applications intéressantes de ce résultat.

1.5.1 Résultat principal.

Etant donné (V_1,ρ_1) et (V_2,ρ_2) deux représentations de G, on note $L_G(V_1,V_2)$ l'ensemble des éléments de $L(V_1,V_2)$ fixes sous l'action de G :

$$L_G(V_1,V_2):=\{u\in L(V_1,V_2)|\quad\forall g\in G,\quad\rho_1(g)\circ u\circ\rho_2(g)^{-1}=u\}$$

Théorème 1.5.1 (Lemme de Schur)**.** *Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations irréductibles de G. Alors :*

(i) *Si (V_1, ρ_1) et (V_2, ρ_2) ne sont pas isomorphes alors $L_G(V_1, V_2) = \{0\}$.*

(ii) *Si $(V_1, \rho_1) = (V_2, \rho_2)$ alors $L_G(V_1, V_2)$ est l'ensemble des homothéties.*

Démonstration. Soit $u \in L_G(V_1, V_2)$. Alors :

$$\forall g \in G, \quad \rho_1(g) \circ u \circ \rho_2(g)^{-1} = u \quad (\star)$$

Il s'ensuit que $\ker(u) \subset V_1$ et $\mathrm{im}(u) \subset V_2$ sont stables sous l'action de G. Ainsi, (V_1, ρ_1) étant irréductible, soit $\ker(u) = \{0\}$ soit $\ker(u) = V_1$ (auquel cas $u = 0$). Donc si $u \neq 0$, alors $\ker(u) = \{0\}$ donc $\mathrm{im}(u) \neq \{0\}$ et ainsi $\mathrm{im}(u) = V_2$ (car (V_2, ρ_2) est irréductible). Mais alors u est injective et surjective donc c'est un isomorphisme. Ce fait et la relation $(\star)$ assurent alors que (V_1, ρ_1) et (V_2, ρ_2) sont isomorphes. D'où (i) par contraposée.

Soit $u \in L_G(V_1, V_1)$. Comme V_1 est un espace vectoriel complexe, u admet une valeur propre λ. Donc $u - \lambda \mathrm{id}_{V_1}$ est de noyeau non nul. Mais $u - \lambda \mathrm{id}_{V_1}$ vérifie $(\star)$ puisqu'une homothétie commute avec tout endomorphisme. Donc le raisonnement précédent assure que $\ker(u - \lambda \mathrm{id}_{V_1})$ est stable par l'action de G. Comme $\ker(u - \lambda \mathrm{id}_{V_1}) \neq \{0\}$ et que (V_1, ρ_1) est irréductible, nécessairement $\ker(u - \lambda \mathrm{id}_{V_1}) = V_1$. Ainsi, u est une homothétie. D'où (ii). □

Etant données deux représentations (V_1, ρ_1) et (V_2, ρ_2) de G et $u \in L(V_1, V_2)$, on défint la moyenne de u par :

$$M(u) := \frac{1}{|G|} \sum_{g \in G} \rho_2(g) \circ u \circ \rho_1(g)^{-1}$$

Lemme 1.5.2. **(i)** *Si (V_1, ρ_1) et (V_2, ρ_2) sont deux représentations irréductibles non isomorphes de G alors pour tout $u \in L(V_1, V_2)$, $M(u) = 0$.*

(ii) *Si (V, ρ) est une représentation irréductible de G et si $u \in L(V)$ alors $M(u) = \frac{Tr(u)}{dim(V)} id_V$.*

(iii) *Si (V, ρ) est une représentation irréductible de G et si $f \in L^2(G)^G$ alors on a l'égalité suivante dans $L(V)$:*

$$\sum_{g \in G} f(g)\rho(g) = \frac{1}{dim(V)} \left(\sum_{g \in G} f(g)\chi_\rho(g) \right) id_V$$

Démonstration. **(i)** On a pour tout $g \in G$:

$$\rho_2(g)M(u)\rho_1(g)^{-1} = \frac{1}{|G|} \sum_{h \in G} \rho_2(g)\rho_2(h)u\rho_1(h)^{-1}\rho_1(g)^{-1} = \frac{1}{|G|} \sum_{h \in G} \rho_2(gh)u\rho_1(gh)^{-1}$$

Comme $h \in G \longmapsto gh \in G$ est une bijection, on obtient par changement d'indice $k := gh$ que :

$$\rho_2(g) \circ M(u) \circ \rho_1(g)^{-1} = \frac{1}{|G|} \sum_{k \in G} \rho_2(k) \circ u \circ \rho_1(k)^{-1} = M(u)$$

Donc $M(u) \in L_G(V_1, V_2)$ et comme (V_1, ρ_1) et (V_2, ρ_2) sont deux représentations irréductibles non isomorphes, le point (i) du lemme de Schur permet de conclure que $M(u) = 0$.

(ii) On avu que $M(u) \in L_G(V, V)$. Ainsi, le point (ii) du lemme de Schur assure que $M(u)$ est une homothétie. Comme toute homothétie, son rapport est égal à $\frac{\mathrm{Tr}(M(u))}{\dim(V)}$. Or, la trace étant un invariant de similitude, on a $\mathrm{Tr}(M(u)) = \mathrm{Tr}(u)$. D'où $M(u) = \frac{\mathrm{Tr}(u)}{\dim(V)} \mathrm{id}_V$.

(iii) Posons $u_f := \sum_{g \in G} f(g)\rho(g)$. $u_f \in L(V)$ comme combinaison linéaire d'éléments de $L(V)$. En outre, pour tout $g \in G$:

$$\rho(g)u_f\rho(g)^{-1} = \sum_{h \in G} f(h)\rho(g)\rho(h)\rho(g)^{-1} = \sum_{h \in G} f(h)\rho(ghg^{-1}) = \sum_{h \in G} f(ghg^{-1})\rho(ghg^{-1})$$

où l'on a utilisé le fait que f est une fonction centrale. Or, $h \in G \longmapsto ghg^{-1} \in G$ est une bijection de réciproque $h \in G \longmapsto g^{-1}hg \in G$ donc par changement d'indice $k := ghg^{-1}$:

$$\rho(g)u_f\rho(g)^{-1} = \sum_{k\in G} f(k)\rho(k) = u_f$$

Donc u_f est invariante sous l'action de G i.e. $u_f \in L_G(V,V)$. Il s'ensuit avec le point (ii) du lemme de Schur que u_f est une homothétie de rapport $\frac{\mathrm{Tr}(u_f)}{\dim(V)}$. Or :

$$\mathrm{Tr}(u_f) = \mathrm{Tr}\left(\sum_{g\in G} f(g)\rho(g)\right) = \sum_{g\in G} f(g)\mathrm{Tr}(\rho(g)) = \sum_{g\in G} f(g)\chi_\rho(g)$$

On a donc bien l'égalité voulue.

□

Théorème 1.5.3 (Frobenius)**.** *Irr(G) est une base orthonormée de l'espace $L^2(G)^G$ des fonctions centrales.*

Démonstration. Soient $\chi_1, \chi_2 \in \mathrm{Irr}(G)$ et (V_1,ρ_1), (V_2,ρ_2) leurs représentations irréductibles respectivement associées. Alors d'après la proposition 1.4.2 :

$$\langle\chi_1,\chi_2\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_1(g)}\chi_2(g) = \frac{1}{|G|}\sum_{g\in G}\chi_{H(\rho_1,\rho_2)}(g) = \mathrm{Tr}\left(\frac{1}{|G|}\sum_{g\in G}H(\rho_1,\rho_2)(g)\right)$$

Or, $\frac{1}{|G|}\sum_{g\in G}H(\rho_1,\rho_2)(g)$ est exactement l'application linéaire de $L(V_1,V_2)$ dans lui même donnée par :

$$M : u \in L(V_1,V_2) \longmapsto M(u) = \frac{1}{|G|}\sum_{g\in G}\rho_2(g)\circ u\circ\rho_1(g)^{-1} \in L(V_1,V_2)$$

Si $\chi_1 \neq \chi_2$ alors (V_1,ρ_1) et (V_2,ρ_2) sont deux représentations irréductibles non isomorphes (car sinon, on aurait $\chi_1 = \chi_2$, comme nous l'avons vu à la remarque 1.4.4). Donc d'après le point (i) du lemme précédent, l'application M est identiquement nulle donc de trace nulle. Ainsi, $\langle\chi_1,\chi_2\rangle = 0$.

Si maintenant, $\chi_1 = \chi_2$ alors on peut supposer que $(V_1,\rho_1) = (V_2,\rho_2)$. Le point (ii) du lemme précédent assure alors que M est l'application :

$$M : u \in L(V_1) \longmapsto \frac{\mathrm{Tr}(u)}{\dim(V)}\mathrm{id}_V \in L(V)$$

C'est le projecteur sur le sous-espace des homothéties parallèlement à l'hyperplan des applications linéaires de trace nulle. M est donc diagonalisable avec deux valeurs propres :

- la valeur propre 1, d'espace propre associé de dimension 1 (le sous-espace des homothéties) ;
- la valeur propre 0, d'espace propre associé de dimension $\dim(V)^2 - 1$ (l'hyperplan des applications linéaires de trace nulle).

Ainsi, on a $\mathrm{Tr}(M) = 1$ et donc $\langle\chi_1,\chi_2\rangle = 1$.

Nous venons ainsi de montrer que Irr(G) est une famille orthonormée de $L^2(G)^G$. Comme $L^2(G)^G$ est de dimension finie, pour montrer que c'est une base, il suffit donc de voir que son supplémentaire orthogonal est réduit à $\{0\}$ dans $L^2(G)^G$. Considérons alors la représentation régulière complexe (V,ρ) de G (décrite dans l'exemple 1.1.6). On peut prendre par exemple $V := \mathbb{C}^G$ dont $(e_g)_{g\in G} := (\delta_g)_{g\in G}$ est une base. On pose alors :

$$\forall g,h \in G, \quad \rho(g)(e_h) := e_{gh}$$

On applique alors le théorème de Maschke (théorème 1.2.5) pour décomposer V en sous-espaces irréduc-

tibles $V = \bigoplus_{i=1}^{r} V_i$. Si $f \in L^2(G)^G$ est orthogonale à $\mathrm{Irr}(G)$, on a alors :

$$\forall i \in \{1, \cdots, r\}, \quad \langle \chi_{\rho_{|V_i}}, f \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} \chi_{\rho_{|V_i}}(g) = 0$$

Comme $\overline{f}$ est une fonction centrale (de même que f), le point (iii) du lemme précédent assure que $\sum_{g \in G} \overline{f(g)} \rho(g)|_{V_i}^{|V_i} = 0$ pour tout $i \in \{1, \cdots, r\}$, de sorte que $\sum_{g \in G} \overline{f(g)} \rho(g) = 0$. En appliquant cette égalité sur e_1 (1 étant le neutre de G), on obtient que :

$$\sum_{g \in G} \overline{f(g)} e_g = 0$$

Or, $(e_g)_{g \in G}$ est libre donc pour tout $g \in G$, $\overline{f(g)} = 0$ i.e. $f = 0$. D'où le résultat. □

Remarque 1.5.4. Si (V_1, ρ_1) et (V_2, ρ_2) sont irréductibles non isomorphes de G alors l'application moyenne M associée est identiquement nulle d'après le point (i) du lemme de Schur. Ainsi, $\mathrm{Tr}(M) = 0$. Or, on a vu dans la preuve du théorème 1.5.3 que $\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle = \mathrm{Tr}(M)$. Ainsi, $\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle = 0$ et donc $\chi_{\rho_1} \neq \chi_{\rho_2}$ d'après le théorème 1.5.3. Nous avons donc montré la réciproque du résultat énoncé à la remarque 1.4.4 dans le cas des représentations irréductibles, ce qui nous permettra de démontrer cette réciproque dans le cas général.

On vient aussi de voir que $\mathrm{Irr}(G)$, l'ensemble des caractères irréductibles s'identifie à l'ensemble des classes de représentations irréductibles de G (modulo la relation d'isomorphisme). A tout caractère $\chi \in \mathrm{Irr}(G)$, on peut donc associer une représentation irréductible (W_χ, ρ_χ) et décrire ainsi toutes les classes susmentionnées.

Enfin, nous venons de prouver que toute fonction centrale $\phi \in L^2(G)^G$ peut être décomposée dans la base $\mathrm{Irr}(G)$ selon la formule :

$$\phi = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi, \phi \rangle \chi$$

appelée *décomposition de Fourier* de ϕ. Les produits scalaires $\langle \chi, \phi \rangle$ seront appelés *coefficients de Fourier* de ϕ.

1.5.2 Applications de l'orthogonalité des caractères.

Pour un groupe fini G, on note $\mathrm{Conj}(G)$ l'ensemble des classes de conjugaison de G.

Corollaire 1.5.5. *On a $|Conj(G)| = |Irr(G)|$. Autrement dit, il y a autant de classes de représentations irréductibles de G (modulo la relation d'isomorphisme) que de classes de conjugaison de G.*

Démonstration. Le théorème 1.5.3 assure que $\dim(L^2(G)^G) = |\mathrm{Irr}(G)|$, l'espace des fonctions centrales de G vers $\mathbb{C}$. Or, la famille $(\mathbb{1}_C)_{C \in \mathrm{Conj}(G)}$ est dans $L^2(G)^G$. Elle est par ailleurs libre puisque les classes de conjugaisons sont disjointes et génératrice de $L^2(G)^G$ car les fonctions centrales sont constantes sur les classes de conjugaison. Ainsi, $|\mathrm{Conj}(G)| = \dim(L^2(G)^G) = |\mathrm{Irr}(G)|$. □

Corollaire 1.5.6. *Soit (V, ρ) une représentation linéaire de G décomposée en somme directes de représentations irréductibles selon le théorème de Maschke $V := \bigoplus_{i=1}^{r} W_i$. Alors pour toute représentation irréductible (W, ρ_W) de G, le nombre de W_i isomorphes à W est égal à $\langle \chi_\rho, \chi_{\rho_W} \rangle$. Ainsi, la décomposition de Maschke de V est essentiellement unique et (V, ρ) est isomorphe à $\left(\prod_{\chi \in Irr(G)} W_\chi^{\langle \chi_\rho, \chi \rangle}, \bigoplus_{\chi \in Irr(G)} \langle \chi_\rho, \chi \rangle \rho_\chi \right)$.*

Démonstration. D'après la proposition 1.3.6, on a :

$$\chi_\rho = \sum_{i=1}^{r} \chi_{\rho_{|W_i}}$$

Donc pour toute représentation irréductible (W, ρ_W) de G :

$$\langle \chi_\rho, \chi_{\rho_W} \rangle = \sum_{i=1}^{r} \langle \chi_{\rho_{|W_i}}, \chi_{\rho_W} \rangle$$

avec $\langle \chi_{\rho_{|W_i}}, \chi_{\rho_W} \rangle = 1$ si et seulement si (W, ρ_W) et $(W_i, \rho_{|W_i})$ sont isomorphes et $\langle \chi_{\rho_{|W_i}}, \chi_{\rho_W} \rangle = 0$ sinon (d'après la remarque 1.5.4). Donc $\langle \chi_\rho, \chi_{\rho_W} \rangle$ est bien le nombre de W_i isomorphes à W. □

Corollaire 1.5.7. *Deux représentations linéaires de degré fini d'un groupe fini G sont isomorphes si et seulement si elles ont même caractère.*

Démonstration. Le sens direct est trivial et a déjà été expliqué en remarque 1.4.4. Réciproquement, si (V, ρ) et (V', ρ') sont deux représentations linéaires de degré fini du groupe fini G alors le corollaire précédent assure qu'elles sont toutes deux isomorphes à $\left(\prod_{\chi \in \mathrm{Irr}(G)} W_\chi^{\langle \chi_\rho, \chi \rangle}, \bigoplus_{\chi \in \mathrm{Irr}(G)} \langle \chi_\rho, \chi \rangle \rho_\chi\right)$ donc isomorphes entre elles. □

Corollaire 1.5.8. *(V, ρ) est une représentation irréductible de G si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

Démonstration. D'après le corollaire précédent, (V, ρ) est isomorphe à :

$$\left(\prod_{\chi \in \mathrm{Irr}(G)} W_\chi^{\langle \chi_\rho, \chi \rangle}, \bigoplus_{\chi \in \mathrm{Irr}(G)} \langle \chi_\rho, \chi \rangle \rho_\chi \right)$$

Ainsi, d'après la proposition 1.3.6 :

$$\chi_\rho = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_\rho, \chi \rangle \chi$$

et par orthogonalité de $\mathrm{Irr}(G)$:

$$\langle \chi_\rho, \chi_\rho \rangle = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_\rho, \chi \rangle^2$$

Or, on sait par le corollaire 1.5.6 que pour tout $\chi \in \mathrm{Irr}(G)$, $\langle \chi_\rho, \chi \rangle$ est le nombre de fois que la représentation irréductible (W_χ, ρ_χ) associée à χ apparaît dans la décomposition de V en sous-représentations irréductibles. Il s'ensuit que (V, ρ) est une représentation irréductible de G si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1$. □

Corollaire 1.5.9 (décomposition de la représentation régulière)**.** *Notons (V_G, ρ_G) la représentation régulière de G.*

- **(i)** *Pour tout $\chi \in Irr(G)$, (W_χ, ρ_χ) apparaît $\langle \chi, \chi_{\rho_G} \rangle = dim(W_\chi)$ fois dans la décomposition de (V_G, ρ_G) en sous-représentations irréductibles.*
- **(ii)** *On a la formule suivante, due à Burnside :*

$$\sum_{\chi \in Irr(G)} dim(W_\chi)^2 = |G|$$

- **(iii)** *Si $g \in G \setminus \{1\}$, alors :*

$$\sum_{\chi \in Irr(G)} dim(W_\chi) \chi(g) = 0$$

Démonstration. On a vu dans l'exemple 1.3.2 que pour tout $g \in G$, $\chi_{\rho_G}(g) = \delta_{g,1}|G|$. Or, d'après le corollaire 1.5.6, pour tout $\chi \in \mathrm{Irr}(G)$, la multiplicité de (W_χ, ρ_χ) dans la décomposition de Maschke de (V_G, ρ_G) vaut :

$$\langle \chi, \chi_{\rho_G} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi_{\rho_G}(g) = \frac{1}{|G|} \overline{\chi(1)} |G| = \mathrm{Tr}(\mathrm{id}_{W_\chi}) = \dim(W_\chi)$$

D'où (i). Ainsi, le corollaire 1.5.6 et la proposition 1.3.6 assurent que :

$$\chi_{\rho_G} = \sum_{\chi \in \mathrm{Irr}(G)} \dim(W_\chi)\chi$$

En appliquant cette égalité en $g = 1$, on aboutit à la formule (ii) et en l'appliquant en $g \in G \setminus \{1\}$, on obtient (iii). □

Corollaire 1.5.10. *Si G est un groupe abélien fini alors toutes ses représentations irréductibles sont de dimension 1 et sont des morphismes de groupes de G vers S^1 (le cercle unité de $\mathbb{C}$).*

Démonstration. Comme G est abélien, toutes les classes de conjugaisons de G sont triviales et donc $|\mathrm{Conj}(G)| = |G|$ donc d'après le corollaire 1.5.5, $|\mathrm{Irr}(G)| = |G|$. Or, d'après la formule de Burnside :

$$\sum_{\chi \in \mathrm{Irr}(G)} \dim(W_\chi)^2 = |G|$$

Et donc nécessairement $\dim(W_\chi) = 1$ pour tout $\chi \in \mathrm{Irr}(G)$. Ainsi, pour tout $\chi \in \mathrm{Irr}(G)$, de représentation associée (W_χ, ρ_χ), et tout $g \in g$, $\chi(g) = \lambda_\chi(g)$ l'unique valeur propre de $\rho_\chi(g)$ donc $\chi(gh) = \lambda_\chi(gh) = \lambda_\chi(g)\lambda_\chi(h) = \chi(g)\chi(h)$ pour tous $g, h \in G$ puisque ρ_χ est un morphisme de groupes. Donc χ est un morphisme de groupes de G vers $\mathbb{C}^*$. Comme G est d'ordre fini, c'est en fait un morphisme de G vers S^1. □

Terminons cette série d'applications par un lemme sur les caractères généralisés. Nous noterons $\|.\|$ la norme associée au produit scalaire $\langle ., . \rangle$.

Lemme 1.5.11. *Soit $\phi \in L^2(G)^G_{\mathbb{Z}}$. Alors :*

- **(i)** $\|\phi\|^2 \in \mathbb{N}$.
- **(ii)** $\|\phi\|^2 = 1$ *si et seulement si* $\phi = \epsilon\chi$ *avec* $\epsilon \in \{-1, 1\}$ *avec* χ *un caractère irréductible.*
- **(iii)** . $\|\phi\|^2 = 2$ *si et seulement si* $\phi = \epsilon\chi - \epsilon'\chi'$ *où* $\epsilon, \epsilon' \in \{-1, 1\}$ *et* χ, χ' *des caractères irréductibles distincts.*

Démonstration. Comme tout caractère est combinaison linéaire entière à coefficients positifs de caractères irréductibles (d'après le théorème de Maschke et la proposition 1.3.6) et comme tout élément de $L^2(G)^G_{\mathbb{Z}}$ est de la forme $\epsilon\chi - \epsilon'\chi'$ où χ et χ' sont des caractères et $\epsilon, \epsilon' \in \{0, 1\}$, on a :

$$\phi = \sum_{\chi \in \mathrm{Irr}(G)} m_\chi \chi$$

avec pour tout $\chi \in \mathrm{Irr}(G)$, $m_\chi \in \mathbb{Z}$. Comme les caractères irréductibles sont orthogonaux (d'après le théorème 1.5.3), on a donc :

$$\|\phi\|^2 = \sum_{\chi \in \mathrm{Irr}(G)} m_\chi^2 \in \mathbb{Z}$$

d'où le point (i). Pour le point (ii), remarquons que $\|\phi\|^2 = 1$ si et seulement si tous les m_χ sont nuls à l'exception d'un seul, qui vaut ± 1. Pour le point (iii), on voit que $\|\phi\|^2 = 2$ si et seulement si tous les m_χ sont nuls à l'exception de deux d'entre eux, qui valent ± 1. □

1.6 Représentations induites.

Pour les questions de résolubilité qui nous intéressent, étudier les sous-groupes d'un groupe fini à l'aide de la théorie des représentations peut être utile. Quels liens y-a-t-il entre les représentations d'un groupe et celles d'un de ses sous-groupes ? Comment passer des unes aux autres ? Ce paragraphe a pour objectif de répondre à ces questions.

On fixe dans donc un groupe fini G et un sous-groupe $H \subset G$. Il est assez simple de restreindre une représentation de G en une représentation de H. Étendre une représentation de H à G tout entier est en revanche plus délicat. Voici comment faire.

Soit (V, ρ) est une représentation linéaire (complexe) de H. On définit alors l'espace vectoriel :

$$\mathrm{Ind}_H^G(V) := \{f \in V^G | \quad \forall (g,h) \in G \times H, \quad f(hg) = \rho(h)(f(g))\}$$

On munit cet espace vectoriel de la représentation $\mathrm{Ind}_H^G(\rho)$ de G donnée pour tous $g \in H$ et $f \in \mathrm{Ind}_H^G(V)$ par :

$$\mathrm{Ind}_H^G(\rho)(g)(f) : x \in G \longmapsto f(xg)$$

Vérifions que $\mathrm{Ind}_H^G(\rho)$ est bien une représentation linéaire de G. Pour tout $g \in G$, $\mathrm{Ind}_H^G(\rho)(g)$ est clairement linéaire de réciproque $\mathrm{Ind}_H^G(\rho)(g^{-1})$ et donc $\mathrm{Ind}_H^G(\rho)$ est à valeurs dans $GL(\mathrm{Ind}_H^G(V))$. Soient $g_1, g_2 \in G$. Alors pour tous $f \in \mathrm{Ind}_H^G(V)$ et $x \in G$:

$$\mathrm{Ind}_H^G(\rho)(g_1g_2)(f)(x) = f(xg_1g_2) = \mathrm{Ind}_H^G(\rho)(g_2)(f)(xg_1) = \mathrm{Ind}_H^G(\rho)(g_1) \circ \mathrm{Ind}_H^G(\rho)(g_2)(f)(x)$$

Ce qui prouve que $\mathrm{Ind}_H^G(\rho)$ est un morphisme de groupes. Ainsi, $(\mathrm{Ind}_H^G(V), \mathrm{Ind}_H^G(\rho))$ est une représentation linéaire de G.

Exemple 1.6.1. Pour $H = \{1\}$ et $(V, \rho) = (\mathbb{C}, 1)$, la représentation triviale de H, la contrainte définissant $\mathrm{Ind}_H^G(V)$ est toujours vérifiée (car 1 agit trivialement) donc $\mathrm{Ind}_H^G(V) = \mathbb{C}^G$. Considérons $(e_g)_{g\in G} := (\delta_{g^{-1}})_{g\in G}$, qui est une base de $\mathbb{C}^G$. Alors pour tous $g, h, x \in G$:

$$\mathrm{Ind}_H^G(\rho)(g)(e_h)(x) = e_h(gx) = \delta_{h^{-1}}(gx) = \delta_{(gh)^{-1}}(x) = e_{gh}(x)$$

Ainsi, $(\mathrm{Ind}_H^G(V), \mathrm{Ind}_H^G(\rho))$ est la représentation régulière de G.

On sait étendre une représentation d'un sous-groupe à un groupe tout entier. Une question naturelle est donc de savoir comment se comportent les caractères lorsque l'on applique le foncteur Ind_H^G.

Théorème 1.6.2. *Soit (V, ρ) une représentation de H et soit $S \subset G$ un système de représentants du quotient $H\backslash G$, l'ensemble des classes à droite de G modulo H (de sorte que $H\backslash G = \{Hs | s \in S\}$ et $G = \bigsqcup_{s\in S} Hs$). Alors :*

$$\chi_{Ind_{H(\rho)}^G}(g) = \sum_{\substack{s\in S \\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1}) = \frac{1}{|H|} \sum_{\substack{s\in G \\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1})$$

Démonstration. Nous allons munir $\mathrm{Ind}_H^G(V)$ d'une base et travailler dans cette base. Soit pour commencer $\mathcal{B} := (e_i)_{1\leq i\leq n}$ une base de V. Comme $G = \bigsqcup_{s\in S} Hs$, pour tout $g \in G$, il existe un unique couple $(h_g, s_g) \in H \times S$ tel que $g = h_g s_g$. On considère alors pour tout $(s, i) \in S \times \{1, \cdots, n\}$:

$$f_{s,i} : g \in G \longmapsto \delta_{s_g,s}\rho(h_g)(e_i) \in V$$

Alors pour $(s, i) \in S \times \{1, \cdots, n\}$ fixé, $f_{s,i} \in \mathrm{Ind}_H^G(V)$. En effet, si $g \in G$ et $h \in H$ alors $s_{hg} = s_g$ et $h_{hg} = hh_g$ donc :

$$f_{s,i}(hg) = \delta_{s_{hg},s}\rho(h_{hg})(e_i) = \delta_{s_g,s}\rho(hh_g)(e_i) = \delta_{s_g,s}\rho(h) \circ \rho(h_g)(e_i) = \rho(h)(f_{s,i})(g)$$

Montrons qu'en fait $\mathcal{C} := (f_{s,i})_{\substack{s\in S \\ 1\leq i\leq n}}$ est une base de $\mathrm{Ind}_H^G(V)$. Soit $(\lambda_{s,i})_{\substack{s\in S \\ 1\leq i\leq n}}$ une famille de complexes

telle que $\sum_{\substack{s\in S\\1\leq i\leq n}} \lambda_{s,i} f_{s,i} = 0$. Evaluons cette égalité en $t \in S$:

$$0 = \sum_{\substack{s\in S\\1\leq i\leq n}} \lambda_{s,i}\delta_{s_t,s}\rho(h_t)(e_i) = \sum_{\substack{s\in S\\1\leq i\leq n}} \lambda_{s,i}\delta_{t,s}\rho(1)(e_i) = \sum_{i=1}^{n} \lambda_{t,i} e_i$$

La liberté de $\mathcal{B}$ permet de conclure que $\lambda_{t,i} = 0$ pour tout $i \in \{1, \cdots, n\}$ et ceci est aussi vrai pour tout $t \in S$. D'où la liberté de $\mathcal{C}$. Si maintenant $f \in \mathrm{Ind}_H^G(V)$ alors pour tout $g \in G$:

$$f(g) = f(h_g s_g) = \rho(h_g)(f(s_g)) = \sum_{i=1}^{n} f(s_g)_i \rho(h_g)(e_i)$$

où $f(s_g)_i$ est la i-ème composante de $f(s_g)$ dans $\mathcal{B}$ pour tout $i \in \{1, \cdots, n\}$. Ainsi :

$$f = \sum_{\substack{s\in S\\1\leq i\leq n}} f(s)_i f_{s,i} \quad (\star)$$

Donc $\mathcal{C}$ est génératrice de $\mathrm{Ind}_H^G(V)$, donc c'est une base de cet espace.

Soit $g \in G$. Alors d'après $(\star)$, la matrice de $\mathrm{Ind}_H^G(\rho)(g)$ s'écrit dans $\mathcal{C}$ sous la forme :

$$\mathrm{Mat}_{\mathcal{C}}\mathrm{Ind}_H^G(\rho)(g) = \left(\mathrm{Ind}_H^G(\rho)(g)(f_{s,i})(t)_j\right)_{\substack{s,t\in S\\1\leq i,j\leq n}} = (f_{s,i}(tg)_j)_{\substack{s,t\in S\\1\leq i,j\leq n}} = (\delta_{s_{tg},s}\rho(h_{tg})(e_i)_j)_{\substack{s,t\in S\\1\leq i,j\leq n}}$$

Ainsi :

$$\chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = \mathrm{Tr}\mathrm{Mat}_{\mathcal{C}}\mathrm{Ind}_H^G(\rho)(g) = \sum_{\substack{s\in S\\1\leq i\leq n}} \delta_{s_{sg},s}\rho(h_{sg})(e_i)_i$$

Or, pour tout $s \in S$, $s_{sg} = s \iff sgs^{-1} \in H$ et alors $h_{sg} = sgs^{-1}$. Donc :

$$\chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \sum_{i=1}^{n} \rho(sgs^{-1})(e_i)_i = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \mathrm{Tr}(\rho(sgs^{-1})) = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1})$$

Puis, comme $G = \bigsqcup_{s\in S} Hs$, on a :

$$\frac{1}{|H|} \sum_{\substack{s\in G\\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1}) = \frac{1}{|H|} \sum_{s\in S} \sum_{\substack{t\in Hs\\ tgt^{-1}\in H}} \chi_\rho(tgt^{-1})$$

mais pour tous $s \in S$ et $t \in Hs$, $s_t = s$ et donc $tgt^{-1} \in H \iff h_t sgs^{-1}h_t^{-1} \in H \iff sgs^{-1} \in H$. Ainsi :

$$\begin{aligned}\frac{1}{|H|} \sum_{\substack{s\in G\\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1}) &= \frac{1}{|H|} \sum_{s\in S} \sum_{\substack{t\in Hs\\ sgs^{-1}\in H}} \chi_\rho(h_t sgs^{-1}h_t^{-1}) = \frac{1}{|H|} \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \sum_{t\in Hs} \chi_\rho(sgs^{-1})\\ &= \frac{1}{|H|} \sum_{\substack{s\in S\\ sgs^{-1}\in H}} |H|\chi_\rho(sgs^{-1}) = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \chi_\rho(sgs^{-1})\end{aligned}$$

D'où le résultat. □

Ce théorème justifie la définition du morphisme entre espaces de fonctions centrales $\mathrm{Ind}_H^G : L^2(H)^H \longrightarrow L^2(G)^G$ donné par la formule :

$$\forall \phi \in L^2(H)^H, \forall g \in G, \quad \mathrm{Ind}_H^G\phi(g) = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \phi(sgs^{-1}) = \frac{1}{|H|} \sum_{\substack{s\in G\\ sgs^{-1}\in H}} \phi(sgs^{-1})$$

qui coincide avec les représentations induites si l'on se restreint aux caractères. On dispose aussi d'un morphisme dans l'autre sens $\mathrm{Res}_G^H : L^2(G)^G \longrightarrow L^2(H)^H$ obtenu en prenant la restriction à H.

Si (V, ρ) est une représentation de G on notera $(V, \mathrm{Res}_G^H(\rho))$ la représentation obtenue en restreignant ρ à H, de sorte que :

$$\chi_{\mathrm{Res}_G^H(\rho)} = \mathrm{Res}_G^H(\chi_\rho)$$

Le théorème 1.6.2 nous donne aussi bien-sûr une formule duale pour Ind_H^G.

Les morphismes Ind_H^G et Res_G^H sont en fait "adjoints" au sens suivant :

Théorème 1.6.3 (formule de réciprocité de Frobenius)**.** *Notons $\langle .,. \rangle_G$ et $\langle .,. \rangle_H$ les produits scalaires sur G et H respectivement. Alors si $\phi_1 \in L^2(H)^H$ et $\phi_2 \in L^2(G)^G$, on a :*

$$\langle Ind_H^G \phi_1, \phi_2 \rangle_G = \langle \phi_1, Res_G^H \phi_2 \rangle_H$$

Démonstration. On sait que :

$$\langle \mathrm{Ind}_H^G \phi_1, \phi_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} \frac{1}{|H|} \left(\sum_{\substack{s \in G \\ sgs^{-1} \in H}} \phi_1(sgs^{-1}) \right) \overline{\phi_2(g)} = \frac{1}{|G||H|} \sum_{\substack{(g,s) \in G^2 \\ sgs^{-1} \in H}} \phi_1(sgs^{-1}) \overline{\phi_2(g)}$$

Or, $\{(g, s) \in G^2 | sgs^{-1} \in H\}$ est en bijection avec $H \times G$ via la bijection $(g, s) \longmapsto (sgs^{-1}, s)$ de réciproque $(h, s) \longmapsto (s^{-1}hs, s)$. Ainsi, par changement d'indice $h = sgs^{-1}$:

$$\begin{aligned} \langle \mathrm{Ind}_H^G \phi_1, \phi_2 \rangle_G &= \frac{1}{|G||H|} \sum_{(h,s) \in H \times G} \phi_1(h) \overline{\phi_2(s^{-1}hs)} = \frac{1}{|G||H|} \sum_{(h,s) \in H \times G} \phi_1(h) \overline{\phi_2(h)} \\ &= \frac{1}{|H|} \sum_{h \in H} \phi_1(h) \overline{\phi_2(h)} = \langle \phi_1, \mathrm{Res}_G^H \phi_2 \rangle_H \end{aligned}$$

où l'on a utilisé le fait que ϕ_2 est centrale. □

1.7 Caractères et théorie algébrique des nombres.

1.7.1 Résultats d'intégralité.

Soit A un anneau. Alors on appelle *G-module sur A* et on note $A[G]$ le A-module A^G. Alors $(\delta_g)_{g \in G}$, la famille des diracs est une A-base de $A[G]$. On aimerait munir $A[G]$ d'une structure de A-algèbre, c'est-à-dire définir un produit interne $\times$ tel que :

$$\forall g, h \in G, \quad \delta_g \times \delta_h = \delta_{gh}$$

Pour un tel produit et pour $\phi, \psi \in A[G]$, on aurait alors :

$$\begin{aligned} \phi \times \psi &= \left(\sum_{g \in G} \phi(g) \delta_g \right) \times \left(\sum_{h \in G} \psi(h) \delta_h \right) = \sum_{g,h \in G} \phi(g)\psi(h) \delta_g \times \delta_h = \sum_{g,h \in G} \phi(g)\psi(h)\delta_{gh} \\ &= \sum_{k \in G} \left(\sum_{\substack{g,h \in G \\ gh = k}} \phi(g)\psi(h) \right) e_k = \sum_{g \in G} \left(\sum_{h \in G} \phi(h)\psi(h^{-1}g) \right) e_g \end{aligned}$$

On définit donc $\phi \times \psi$ comme la fonction :

$$\phi \times \psi : g \in G \longmapsto \sum_{h \in G} \phi(h)\psi(h^{-1}g)$$

On peut vérifier que muni d'un tel produit (qui est en fait le produit de convolution), $A[G]$ est bien une A-algèbre.

Supposons désormais que A est un corps et notons $K := A$. Si (V, ρ) est une représentation de G de corps de base K alors on dispose d'un unique morphisme de K-algèbre :

$$\Phi_\rho : K[G] \longrightarrow L(V)$$

tel que $\Phi_\rho(\delta_g) = \rho(g)$ pour tout $g \in G$. Un tel morphisme est appelé *G-morphisme.*

On commence par énoncer un résultat d'intégralité des caractères tout à fait central qui jouera un rôle majeur dans les preuves des théorèmes de Burnside (partie 2) et de Suzuki (partie 3).

Théorème 1.7.1. *Soit (V, ρ) une représentation irréductible de G. Alors pour tout $g \in G$, $\frac{|C_G(g)|}{dim(V)}\chi_\rho(g)$ est un entier algébrique, $C_G(g) := \{hgh^{-1} | h \in G\}$ étant la classe de conjugaison de g dans G.*

Démonstration. Considérons l'endomorphisme $u := \sum_{h \in C_G(g)} \rho(h) \in L(V)$. Alors pour tout $k \in G$:

$$\rho(k) \circ u \circ \rho(k)^{-1} = \sum_{h \in C_G(g)} \rho(k) \circ \rho(h) \circ \rho(k)^{-1} = \sum_{h \in C_G(g)} \rho(khk^{-1})$$

Or $kC_G(g)k^{-1} \subset C_G(g)$ de sorte que $h \in C_G(g) \longmapsto khk^{-1}$ induise une bijection de $C_G(g)$ dans lui-même, ce qui légitime le changement d'indice $h' := khk^{-1}$ et donne :

$$\rho(k) \circ u \circ \rho(k)^{-1} = \sum_{h' \in C_G(g)} \rho(h') = u$$

Donc $u \in L_G(V, V)$ et le lemme de Schur assure alors que $u = \frac{\mathrm{Tr}(u)}{\dim(V)}\mathrm{id}_V = \frac{|C_G(g)|}{\dim(V)}\chi_\rho(g)\mathrm{id}_V$. Ainsi, pour que $\frac{|C_G(g)|}{\dim(V)}\chi_\rho(g)$ soit entier algébrique, il faut et il suffit que u admette un polynôme annulateur à coefficients entiers.

Pour montrer cela, travaillons dans $\mathbb{C}[G]$. On considère $a := \sum_{h \in C_G(g)} \delta_h \in \mathbb{Z}[G]$, de sorte que $\Phi_\rho(a) = u$. Il suffit donc de trouver un polynôme annulateur de a dans $\mathbb{Z}[G]$. On considère R le sous-$\mathbb{Z}$-module de $\mathbb{Z}[G]$ engendré par $(a^n)_{0 \leq n \leq |G|}$. Comme $\mathbb{Z}[G] \subset \mathbb{R}[G]$, on peut considérer E, le sous-$\mathbb{R}$-espace vectoriel de $\mathbb{R}[G]$ engendré par R. Ainsi, R est un sous-groupe additif de E, R engendre E et enfin, R est discret dans E car $R \subset \mathbb{Z}[G]$, qui est discret dans $\mathbb{R}[G]$. Donc R est un réseau de E et par suite, il admet une $\mathbb{Z}$-base d'après le théorème 2.4 du polycopié de cours et toute $\mathbb{Z}$-base de R est de cardinal $\leq \dim_{\mathbb{R}}(E) \leq \dim_{\mathbb{R}}\mathbb{R}[G] = |G|$ d'après la proposition 2.9 du même document. Si par l'absurde $(a^n)_{0 \leq n \leq |G|}$ était $\mathbb{Z}$-libre alors ce serait une $\mathbb{Z}$-base de R à $|G|+1$ éléments (car cette famille est génératrice), ce qui est impossible. Ainsi, $(a^n)_{0 \leq n \leq |G|}$ est $\mathbb{Z}$-liée donc on dispose de $P \in \mathbb{Z}[X]$ non nul de degré $\leq |G|$ annulant a dans $\mathbb{Z}[G]$. On a alors :

$$P(u) = P(\Phi_\rho(a)) = \Phi_\rho(P(a)) = \Phi_\rho(0) = 0$$

D'où le résultat. □

Corollaire 1.7.2. *Soit (V, ρ) une représentation irréductible de G. Alors $dim(V)$ divise $|G|$.*

Démonstration. D'après le théorème de Frobenius (théorème 1.5.3), comme χ_ρ est irréductible on a :

$$\sum_{g \in G} |\chi_\rho(g)|^2 = |G|\langle \chi_\rho, \chi_\rho \rangle = |G|$$

Soient $g_1, \cdots, g_k$ des représentants de toutes les classes de conjugaison de G tous dans des classes distinctes. Alors comme χ_ρ est une fonction centrale, on peut réécrire cette égalité en :

$$|G| = \sum_{i=1}^{k} \sum_{h \in C_G(g_k)} |\chi_\rho(h)|^2 = \sum_{i=1}^{k} \sum_{h \in C_G(g_i)} |\chi_\rho(g_i)|^2 = \dim(V) \sum_{i=1}^{k} \frac{|C_G(g_i)|}{\dim(V)} \chi_\rho(g_i)\overline{\chi_\rho(g_i)}$$

On sait que l'ensemble des entiers algébriques est un sous-anneau de l'ensemble des entiers algébriques $\overline{\mathbb{Q}}$. Ainsi les sommes et les produits d'entiers algébriques sont des entiers algébriques. Ainsi, pour tout $k \in \{1, \cdots, k\}$, comme $\overline{\chi_\rho(g_i)}$ est (d'après la remarque 1.3.3) somme de racines de l'unité (qui sont des entiers algébriques), c'est un entier algébrique. Ainsi, d'après le théorème précédent, $\frac{|G|}{\dim(V)} = \sum_{i=1}^{k} \frac{|C_G(g_i)|}{\dim(V)} \chi_\rho(g_i)\overline{\chi_\rho(g_i)}$ est un entier algébrique comme somme de produits d'entiers algébriques. Or, c'est un rationnel. Donc d'après la proposition 1.14 du polycopié de cours, c'est un entier. Ainsi, $\dim(V)||G|$. □

1.7.2 Action du groupe de galois $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les caractères.

Soit χ un caractère de G. Alors on peut trouver un morphisme de groupes $\rho : G \longrightarrow GL_n(\mathbb{C})$ tel que :

$$\forall g \in G, \quad \chi(g) = \mathrm{Tr}(\rho(g))$$

en prenant par exemple la matrice d'une représentation de G de caractère χ dans une base donnée. Réciproquement, un tel morphisme de groupes $G \longrightarrow GL_n(\mathbb{C})$ définit trivialement une représentation de G dans l'espace vectoriel $\mathbb{C}^n$.

Nous avons vu que pour tout $g \in G$, $\chi(g)$ est un entier algébrique (comme somme de racines $|G|$-ièmes de l'unité). Il est donc aisé de faire agir $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur χ en définissant χ^σ par $\chi^\sigma(g) := \sigma(\chi(g))$ pour tous $g \in G$ et $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, χ^σ est-il toujours un caractère ? La réponse est oui.

Lemme 1.7.3. *Pour tout $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, χ^σ est le caractère d'une représentation de G de même dimension que toute représentation associée à χ.*

Démonstration. Soit $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Alors σ peut être étendu à $\mathbb{C}$ tout entier d'après le théorème de plongement des morphismes (théorème 3.9.1. de [Galois]). Notons $\tilde{\sigma}$ un tel prolongement de σ. A toute matrice $M \in M_n(\mathbb{C})$, on peut associer $M^{\tilde{\sigma}} := (\tilde{\sigma}(M_{i,j}))_{1 \leq i,j \leq n}$. Si $M \in GL_n(\mathbb{C})$ alors $\det(M^{\tilde{\sigma}}) = \tilde{\sigma}(\det(M)) \neq 0$ et donc $M^{\tilde{\sigma}} \in GL_n(\mathbb{C})$. Ainsi :

$$\rho^{\tilde{\sigma}} : g \in G \longmapsto \rho(g)^{\tilde{\sigma}} \in GL_n(\mathbb{C})$$

est bien définie. Par propriété de morphisme de corps de $\tilde{\sigma}$, on obtient que $\rho^{\tilde{\sigma}}$ est toujours un morphisme de groupes donc une représentation de dimension n de G et que de plus :

$$\forall g \in G, \quad \chi_{\rho^{\tilde{\sigma}}}(g) = \mathrm{Tr}(\rho(g)^{\tilde{\sigma}}) = \sigma(\mathrm{Tr}(\rho(g))) = \sigma(\chi(g))$$

Donc $\chi^{\tilde{\sigma}}$ est bien le caractère d'une représentation de G de dimension n égale à la dimension que toute représentation associée à χ (d'après le corollaire 1.5.7). □

2 Une première application de la théorie des caractères : le théorème de Frobenius.

On prouve ici un premier résultat non-trivial de théorie des groupes à l'aide de la théorie des caractères. C'est l'occasion d'en voir toute la puissance.

2.1 Deux versions d'un même énoncé.

Définition 2.1.1. *Un groupe fini G est dit* de Frobenius *lorsqu'il existe un sous-groupe $H \subset G$ tel que pour tout $g \in G \setminus H$, $gHg^{-1} \cap H = \{1\}$. Un tel sous-groupe H est appelé* complément de Frobenius.

Exemple 2.1.2. Soit $G := GA(\mathbb{F}_q)$, le groupe affine du corps fini à q éléments $\mathbb{F}_q$ formé par les applications de la forme $x \in \mathbb{F}_q \longmapsto ax + b \in \mathbb{F}_q$ avec $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$. C'est bien un groupe pour la composition et il est en fait de Frobenius. Prenons comme complément de Frobenius le sous-groupe $H := GL(\mathbb{F}_q)$ formé par les applications linéaires. Alors pour tout $h : x \longmapsto ax$ dans H et $g : x \longmapsto bx + c$ dans $G \setminus H$ ($c \neq 0$), on a $g^{-1} : x \longmapsto b^{-1}(x - c)$ et donc :

$$\forall x \in \mathbb{F}_q, ghg^{-1}(x) = bab^{-1}(x - c) + c = ax + c(1 - a)$$

Donc $ghg^{-1} \in H$ si et seulement si $a = 1$ et ainsi $gHg^{-1} \cap H = \{\mathrm{id}_{\mathbb{F}_q}\}$.

On peut voir que le complément H n'est pas unique ici car l'ensemble des applications affines fixant un point $x_0 \in \mathbb{F}_q$ convient aussi (nous venons de traiter le cas $x_0 = 0$).

Il y a en fait deux versions différentes et équivalentes du théorème de Frobenius. La première est un résultat général sur les groupes de Frobenius.

Théorème 2.1.3 (Frobenius, version 1)**.** *Soit G un groupe de Frobenius et H un complément de Frobenius de G. Alors il existe un sous-groupe distingué K de G tel que $G = K \rtimes H$.*

Exemple 2.1.4. On peut voir aisément que ceci est vrai dans $G := GA(\mathbb{F}_q)$. En effet, avec $H := GL(\mathbb{F}_q)$ on peut prendre le sous-groupe des translations :

$$K := \{x \in \mathbb{F}_q \longmapsto x + b \in \mathbb{F}_q | b \in \mathbb{F}_q\}$$

On a alors clairement $G = KH$ puisque toute application $g : x \longmapsto ax + b$ de G est la composée de $x \longmapsto ax$ et de $x \longmapsto x + b$. En outre, il est immédiat que $H \cap K = \{\mathrm{id}_{\mathbb{F}_q}\}$. Enfin, K est distingué dans G car pour tout $k : x \longmapsto x + b$ dans K et $g : x \longmapsto cx + d$ dans G, on a $g^{-1} : x \longmapsto c^{-1}(x - d)$ et donc :

$$\forall x \in \mathbb{F}_q, \quad gkg^{-1}(x) = c(c^{-1}(x - d) + b) + d = x + bc$$

de sorte que $gkg^{-1} \in K$. Ainsi, $G = K \rtimes H$ par définition.

La seconde version n'a pas de lien apparent avec les groupes de Frobenius mais s'y ramène en fait assez bien comme nous le verrons bientôt. C'est une reformulation plus explicite et appliquée de la première version.

Théorème 2.1.5 (Frobenius, version 2)**.** *Soit G un groupe agissant transitivement*[3] *sur un ensemble X tel que pour tout élément non trivial de G fixe au plus un point de X. Alors l'ensemble des éléments de G sans point fixe forme, avec le neutre 1, un sous-groupe de G.*

Exemple 2.1.6. Il est clair que $G := GA(\mathbb{F}_q)$ agit transitivement sur $X := \mathbb{F}_q$ (tout élément $x \in \mathbb{F}_q$ étant dans l'orbite de 0 car il suffit de translater par x pour envoyer 0 sur x). En outre, tout élément

3. C'est à dire qu'il n'y a qu'une seule orbite sous l'action de G. Pour un élément $x \in X$ quelconque $G \bullet x = X$.

non trivial de G fixe au plus un point (car sinon on aurait un polynôme d'ordre 1 à deux racines, ce qui est impossible dans un corps). En outre, l'ensemble des éléments sans point fixe de G est l'ensemble $K \setminus \{\mathrm{id}_{\mathbb{F}_q}\}$ des translations non triviales de $\mathbb{F}_q$. Or, K est un sous-groupe de G. La version 2 du théorème de Frobenius est donc aussi vérifiée dans $GA(\mathbb{F}_q)$.

À la lumière de cet exemple, il est raisonnable de penser que les deux versions du théorème de Frobenius sont équivalentes. Prouvons-le.

Démonstration. (équivalence des deux versions du théorème de Frobenius)

$\Longrightarrow$ Supposons la version 1 du théorème vérifiée. Soient G un groupe et X un ensemble vérifiant les hypothèses de la version 2. Nous allons montrer qu'en fait G est de Frobenius. Pour tout $x \in X$, on considère le stabilisateur de x :

$$G_x := \{g \in G | g \bullet x = x\}$$

G_x est un sous-groupe de G. Et en outre pour tout $g, h \in G$:

$$h \in G_{g\bullet x} \Longleftrightarrow (hg) \bullet x = g \bullet x \Longleftrightarrow (g^{-1}hg) \bullet x = x \Longleftrightarrow g^{-1}hg \in G_x \Longleftrightarrow h \in gG_xg^{-1}$$

De sorte que $G_{g\bullet x} = gG_xg^{-1}$. Pour $x \in X$ fixé et $g \in G \setminus G_x$ $(g \bullet x \neq x)$, $gG_xg^{-1} \cap G_x = G_{g\bullet x} \cap G_x = \{1\}$ puisqu'aucun élément non trivial de G ne stabilise deux éléments distincts de X. Ainsi, G est de Frobenius et G_x est un complément de Frobenius de G. D'après la version 1 du théorème de Frobenius, on dispose donc de K_x un sous-groupe distingué de G tel que $G = K_x \rtimes H_x$, de sorte que $K_x \cap G_x = \{1\}$. Ainsi :

$$\bigcap_{x\in X} K_x = G \setminus \bigcup_{x\in X} G_x \cup \{1\}$$

est un sous-groupe de G. Or, c'est exactement l'ensemble formé par le neutre 1 et tous les éléments sans point fixe de G. D'où la version 2 du théorème de Frobenius.

$\Longleftarrow$ Supposons la version 2 du théorème vérifiée. Soient G un groupe de Frobenius et H un complément de Frobenius de G. Nous allons construire un ensemble X sur lequel G agit selon les hypothèses de la version 2 du théorème. Prenons pour X l'ensemble quotient $H \setminus G = \{Hg | g \in G\}$ des classes à droite de G modulo H. On fait agir G sur $H \setminus G$ par multiplication à droite :

$$\forall g, g' \in G, \quad g \bullet Hg' := Hg'g$$

Prouvons alors le lemme suivant.

Lemme 2.1.7. *L'action de G sur $H\setminus G$ est transitive et tout élément non trivial de G fixe au plus un point de $H \setminus G$. Pour tout $g \in G$, le stabilisateur de Hg est $G_{Hg} = g^{-1}Hg$ et ces ensembles ne s'intersectent donc qu'en* 1*. Finalement, si S est un ensemble de représentants décrivant injectivement $H \setminus G$ et si K est l'ensemble formé par* 1 *ainsi que tous les éléments sans point fixe de G, on a la partition :*

$$G = \{1\} \sqcup \bigsqcup_{s\in S} (s^{-1}Hs \setminus \{1\}) \sqcup (K \setminus \{1\})$$

Et $|K| = \frac{|G|}{|H|}$.

Démonstration. (du lemme) L'action de G sur $H \setminus G$ est trivialement transitive. De plus, pour tous $Hg \in H \setminus G$ et $g' \in G$, on a $g' \in G_{Hg} \Longleftrightarrow Hgg' = Hg \Longleftrightarrow g' \in g^{-1}Hg$ donc $G_{Hg} = g^{-1}Hg$. Si Hg et Hg' sont deux éléments distincts de $H \setminus G$ alors :

$$G_{Hg} \cap G_{Hg'} = g^{-1}Hg \cap g'^{-1}Hg' = g^{-1}(H \cap (g'g^{-1})^{-1}Hg'g^{-1})g = g^{-1}\{1\}g = \{1\}$$

vu que H est complément de Frobenius de G et que $g'g^{-1} \in H \setminus G$ car $Hg \neq Hg'$. Ainsi, tout élément non trivial de G est dans un stabilisiteur au plus donc fixe au plus un élément. La partition énoncée dans le lemme est donc évidente. En passant aux cardinaux dans cette partition, on obtient que :

$$|G| = |S|(|H| - 1) + |K|$$

Comme $|S| = \frac{|G|}{|H|}$, on en déduit alors que $|K| = \frac{|G|}{|H|}$. □

D'après la version 2 du théorème, l'ensemble K formé par 1 et les éléments sans point fixe de G est un sous-groupe de G. Ce sous-groupe est distingué dans G car si $k \in K \setminus \{1\}$, $g \in G$ et $Hg_1 \in H \setminus G$ vérifient $Hg_1gkg^{-1} = Hg_1$ alors k fixe Hg_1g, ce qui est impossible. Donc $gkg^{-1} \in K$.

Soit $\phi : (k, h) \in K \times H \longmapsto kh \in G$. Alors si $(k, h) \in K \times H$ vérifie $\phi(k, h) = 1$, on a $k = h^{-1} \in H$ et donc $k = 1$ et $h = 1$ car $H \cap K = \{1\}$. Donc ϕ est injective. Or, nous venons de voir que $|K \times H| = |G|$. Ainsi, ϕ est surjective, $G = KH$ et ainsi $G = K \rtimes H$. D'où la version 1 du théorème. □

2.2 Preuve du théorème de Frobenius.

Nous prouvons en fait la première version du théorème de Frobenius. On fixe G un groupe de Frobenius et H un complément de G. La preuve repose sur le lemme essentiel suivant :

Lemme 2.2.1. *Si (V, ρ) est une représentation irréductible de H alors il existe $(\tilde{V}, \tilde{\rho})$ une représentation irréductible de G telle que (V, ρ) soit isomorphe à $(\tilde{V}, Res^H_G \tilde{\rho})$ et dont le caractère $\chi_{\tilde{\rho}}$ est constant égal à $dim(V)$ sur $K := G \setminus \bigcup_{g \in G}(g^{-1}Hg \setminus \{1\})$.*

Démonstration. D'après le lemme 2.1.7 on a la partition :

$$G = \{1\} \sqcup \bigsqcup_{s \in S} (s^{-1}Hs \setminus \{1\}) \sqcup (K \setminus \{1\}) \quad (\star)$$

où S est un ensemble de représentants de $H \setminus G$ et où K désigne l'ensemble formé par 1 et tous les éléments de G sans point fixe lorsqu'ils agissent naturellement sur $H \setminus G$ ($s^{-1}Hs$ étant le stabilisateur de Hs pour tout $s \in S$). On a aussi vu que $|K| = \frac{|G|}{|H|}$ en utilisant la partition $(\star)$.

Le théorème 1.6.2 assure que :

$$\forall g \in G, \quad \chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = \mathrm{Ind}_H^G(\chi_\rho)(g) = \sum_{\substack{s \in S \\ sgs^{-1} \in H}} \chi_\rho(sgs^{-1}) = \sum_{\substack{s \in S \\ g \in s^{-1}Hs}} \chi_\rho(sgs^{-1}) \quad (\star\star)$$

Donc si $g = 1$:

$$\chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = \sum_{\substack{s \in S \\ 1 \in H}} \chi_\rho(1) = |S|\dim(V) = \frac{|G|}{|H|}\dim(V)$$

Si $g \in K \setminus \{1\}$, g n'est dans aucun des $s^{-1}Hs$ (pour $s \in S$) donc $\chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = 0$. Enfin, si g est dans l'un des $s^{-1}Hs \setminus \{1\}$ pour $s \in S$ alors $\chi_{\mathrm{Ind}_{H(\rho)}^G}(g) = \chi_\rho(sgs^{-1})$.

Ainsi :

$$\begin{aligned}\sum_{g \in G \setminus K} |\chi_{\mathrm{Ind}_{H(\rho)}^G}(g)|^2 &= \sum_{s \in S} \sum_{g \in s^{-1}Hs \setminus \{1\}} |\chi_{\mathrm{Ind}_{H(\rho)}^G}(g)|^2 = \sum_{s \in S} \sum_{sgs^{-1} \in H \setminus \{1\}} |\chi_\rho(sgs^{-1})|^2 \\ &= \sum_{s \in S} \sum_{h \in H \setminus \{1\}} |\chi_\rho(h)|^2 = \sum_{s \in S} (|H|\langle \chi_\rho, \chi_\rho \rangle - \chi_\rho(1))\end{aligned}$$

Or, comme (V, ρ) est irréductible, $\langle \chi_\rho, \chi_\rho \rangle = 1$ donc :

$$\sum_{g \in G \setminus K} |\chi_{\mathrm{Ind}_{H(\rho)}^G}(g)|^2 = |S|(|H| - \dim(V)^2) = \frac{|G|}{|H|}(|H| - \dim(V)^2) \quad (\star\star)$$

En considérant la représentation triviale de H, donnée par l'identité sur le $\mathbb{C}$-espace vectoriel $\mathbb{C}$, on obtient que l'application constante égale à 1 est un caractère de H. On peut donc considérer $\mathrm{Ind}_H^G(1)$, qui est toujours un caractère et qui vaut, par les mêmes argumens que ceux donnés pour $\chi_{\mathrm{Ind}_{H(\rho)}^G}$:

— $\frac{|G|}{|H|}$ en 1 ;
— 0 sur $K \setminus \{1\}$;
— 1 sur $G \setminus K$.

On considère le caractère généralisé de G :

$$\phi := \chi_{\mathrm{Ind}_{H(\rho)}^G} - \dim(V)\mathrm{Ind}_H^G(1) + \dim(V)$$

D'après les discussions précédentes sur les valeurs de $\chi_{\mathrm{Ind}_{H(\rho)}^G}$ et $\mathrm{Ind}_H^G(1)$, $\phi(g) = \dim(V)$ si $g \in K$ et $\phi(g) = \chi_{\mathrm{Ind}_{H(\rho)}^G}(g)$ si $g \in G \setminus K$. Ainsi, par $(\star\star)$:

$$\begin{aligned}\langle \phi, \phi \rangle &= \frac{1}{|G|} \sum_{g \in G} |\phi(g)|^2 = \frac{1}{|G|} \left(\frac{|G|}{|H|}(|H| - \dim(V)^2) + \dim(V)^2 |K| \right) \\ &= \frac{1}{|G|} \left(\frac{|G|}{|H|}(|H| - \dim(V)^2) + \dim(V)^2 \frac{|G|}{|H|} \right) = 1\end{aligned}$$

Si le lecteur se demande pourquoi ce caractère généralisé ϕ a été introduit, la réponse tient dans cette égalité qui en fait un caractère irréductible. En effet, d'après le lemme 1.5.11, ϕ vaut donc $\epsilon\chi_{\tilde{\rho}}$ où $(\tilde{V}, \tilde{\rho})$ est une représentation irréductible de G et $\epsilon \in \{-1, 1\}$. Comme $\phi(1) = \dim(V) > 0$ et $\chi_{\tilde{\rho}}(1) = \dim(\tilde{V}) > 0$, $\epsilon = 1$ et donc $\phi = \chi_{\tilde{\rho}}$. L'idée de cette preuve était de modifier la représentation induite pour obtenir cela. Si on considère la forme de la modification, on s'aperçoit que c'est relativement analogue à l'introduction d'une constante modulo une fonction « indicatrice » du sous groupe induit, donc assez naturelle. Après cette digression, continuons. On a :

$$\chi_{\mathrm{Res}_{G(\tilde{\rho})}^H} = \mathrm{Res}_G^H(\chi_{\tilde{\rho}}) = \mathrm{Res}_G^H(\phi) = \mathrm{Res}_G^H(\chi_{\mathrm{Ind}_{H(\rho)}^G}) = \chi_\rho$$

la dernière égalité venant de $(\star\star)$ et du fait que H est un complément de Frobenius de G. Donc d'après le corollaire 1.5.7, (V, ρ) est isomorphe à $(\tilde{V}, \mathrm{Res}_G^H(\tilde{\rho}))$.

□

Soit (V_H, ρ_H) la représentation régulière de H. Alors d'après le corollaire 1.5.9, on a :

$$\chi_{\rho_H} = \sum_{\chi \in \mathrm{Irr}(H)} \dim(W_\chi)\chi$$

Soit :

$$\tilde{\chi}_{\rho_H} := \sum_{\chi \in \mathrm{Irr}(H)} \dim(W_\chi)\tilde{\chi}$$

où pour tout $\chi \in \mathrm{Irr}(H)$, $\tilde{\chi}$ est le caractère associé à χ selon le procédé du lemme précédent, qui étend en particulier χ à G (en plus d'être associé à une représentation irréductible de G dont la restriction à H est isomorphe à toute représentation de caractère χ). D'après la proposition 1.3.6, $\tilde{\chi}_{\rho_H}$ est un caractère. En outre, $\mathrm{Res}_G^H \tilde{\chi}_{\rho_H} = \chi_{\rho_H}$. Ainsi, $\tilde{\chi}_{\rho_H}$ s'annule sur $H \setminus \{1\}$ et sur tous ses conjugués car c'est une fonction centrale. Comme $G = \bigcup_{g \in G}(g^{-1}Hg \setminus \{1\}) \sqcup K$, on en déduit que $\tilde{\chi}_{\rho_H}$ est à support dans K. Or, d'après le lemme précédent, toutes les $\tilde{\chi}$ pour $\chi \in \mathrm{Irr}(H)$ sont constantes égales à $\dim(W_\chi)$ sur K. Ainsi, $\tilde{\chi}_{\rho_H}$ est constante égale à $\tilde{\chi}_{\rho_H}(1)$ sur K. Donc K est le noyau du caractère $\tilde{\chi}_{\rho_H}$ et d'après le point (iv) de la proposition 1.3.4, c'est un sous-groupe distingué de G. Le fait que $K \cap H = \{1\}$ est immédiat et le fait que $KH = G$ se démontre par un argument de cardinalité analogue à celui donné dans la preuve de l'équivalence entre les deux versions du théorème de Fobenius (sens réciproque). Donc $G = K \rtimes H$. On a donc montré le théorème de Frobenius (version 1).

3 Une deuxième application de la théorie des caractères : le théorème de Burnside.

On présente et prouve ici un premier résultat de résolubilité obtenu de façon assez concise avec la théorie des caractères.

Théorème 3.0.1 (Burnside, 1905)**.** *Tout groupe de cardinal admettant au plus deux facteurs premiers est résoluble.*

Pour rappel, un groupe G est dit *résoluble* lorsqu'il existe une suite de sous-groupes $G_0 := \{1\} \subsetneq G_1 \subsetneq \cdots \subsetneq G_{n-1} \subsetneq G_n := G$ telle que tout tout $i \in \{0, \cdots, n-1\}$, G_i est distingué dans G_{i+1} et G_{i+1}/G_i est abélien. On rappelle aussi le résultat essentiel (et intuitif) suivant qui nous permettra de raisonner par récurrence sur le cardinal du groupe dans la preuve du théorème de Burnside.

Proposition 3.0.2. *Soient G un groupe et H un sous-groupe distingué de G. Si H et G/H sont résolubles alors G est résoluble.*

3.1 Une première idée de preuve

Pour donner une idée de la preuve du lemme de Burnside, on peut commencer par prouver un cas particulier et voir comment la preuve se généralise.

Proposition 3.1.1. *Tout groupe dont le cardinal est une puissance de nombre premier est résoluble.*

Démonstration. Soit p un nombre premier. On montre par récurrence sur $\alpha \in \mathbb{N}$ que tout groupe d'ordre p^α est résoluble.

Le groupe trivial $G = \{1\}$ est trivialement résoluble donc le cas $\alpha = 0$ est vérifié.

Soit maintenant $\alpha \in \mathbb{N}^*$. Supposons le résultat vrai aux rangs $\leq \alpha - 1$. Soit G un groupe de cardinal p^α. Il s'agit de montrer que $Z(G)$, le centre de G, est non trivial. Comme $Z(G)$ est abélien et que c'est un sous-groupe distingué de G, il suffira d'appliquer l'hypothèse de récurrence à $G/Z(G)$ (qui est une puissance de p d'exposant $\leq \alpha - 1$ d'après le théorème de Lagrange et vu que $Z(G)$ est non trivial), puis de conclure par la proposition 3.0.2. Nous sommes donc bien ramenés à montrer que $Z(G)$ est non trivial. Pour cela faisons agir G sur lui même par conjugaison. Soient $g_0 := 1, g_1, \cdots, g_k$ des représentants de toutes les classes de conjugaison de G (décrivant injectivement ces classes). Alors l'équation aux classes assure que :

$$p^\alpha = |G| = |C_G(1)| + \sum_{i=1}^{k} |C_G(g_i)| = 1 + \sum_{i=1}^{k} \frac{|G|}{|G_{g_i}|} \quad (\star)$$

Ainsi, toutes les $|C_G(g_i)| = \frac{|G|}{|G_{g_i}|}$ sont des puissances de p. Si par l'absurde aucun des cardinaux $|C_G(g_i)|$ pour $i \geq 1$ n'était égal à 1 alors p diviserait $\sum_{i=1}^{k} |C_G(g_i)|$ et p^α don 1 d'après $(\star)$ ce qui est absurde. Donc on dispose de $g \in G \setminus \{1\}$ tel que $|C_G(g)| = 1$. Donc g commute avec tout élément de G. Il s'ensuit que $Z(G)$ est non trivial comme annoncé. D'où l'itération et le résultat. □

On voit que dans la preuve précédente, l'argument principal est l'équation aux classes $(\star)$ qui permet d'obtenir un résultat sur les cardinaux des classes de conjugaison. Essayons d'adapter cet argument dans le cas où le groupe G est de cardinal $p^\alpha q^\beta$ pour $\alpha, \beta \in \mathbb{N}^*$. Soient $g_0 := 1, g_1, \cdots, g_k$ des représentants de toutes les classes de conjugaison de G décrivant injectivement ces classes. Alors :

$$p^\alpha q^\beta = |G| = 1 + \sum_{i=1}^{k} |C_G(g_i)| = 1 + \sum_{i=1}^{k} \frac{|G|}{|G_{g_i}|}$$

Tous les $|C_G(g_i)| = \frac{|G|}{|G_{g_i}|}$ pour $i \geq 1$ sont des produits de puissances de p et de q et si par l'absurde q était un facteur de tous les $|C_G(g_i)|$, alors on obtiendrait que $q|1$. On obtient donc que l'un des $|C_G(g_i)|$

est une puissance de p pour $i \geq 1$... Et l'on ne peut pas conclure que $|C_G(g_i)| = 1$ et donc que $Z(G)$ est non trivial pour autant. C'est même faux en général :

Exemple 3.1.2. $\mathfrak{S}_3$ est d'ordre $6 = 2 \times 3$ et ne contient que l'identité, 3 transpositions et 2 3-cycles qui forment ses trois classes de conjugaison. Il n'y a donc aucune classe de conjugaison autre que $\{\mathrm{id}_{\{1,2,3\}}\}$ qui soit triviale dans $\mathfrak{S}_3$. Ceci montre en particulier que $Z(\mathfrak{S}_3)$ est trivial.

On peut être déçus certes, mais pas désemparés pour autant. En effet, la théorie des caractères nous permet de conclure à partir de l'existence de $g \in G \setminus \{1\}$ tel que $|C_G(g)|$ soit une puissance de p.

3.2 La théorie des caractères à la rescousse.

Lemme 3.2.1. *Soient $\lambda_1, \cdots, \lambda_n$ des racines de l'unité. Alors $z := \frac{1}{n}\sum_{i=1}^n \lambda_i$ est entier algébrique si et seulement si $a = 0$ ou $\lambda_1 = \cdots = \lambda_n = a$.*

Démonstration. Remarquons tout d'abord que a est algébrique sur $\mathbb{Q}$ comme combinaison $\mathbb{Q}$-linéaire de nombres algébriques sur $\mathbb{Q}$. Notons donc $a_1 = a, \cdots, a_k$ les $\mathbb{Q}$-conjugués de a et N l'ordre maximal des λ_i. Alors tous les λ_i sont dans $K := \mathbb{Q}(e^{\frac{2i\pi}{N}})$ et il en est donc de même pour a et ses $\mathbb{Q}$-conjugués. Ainsi, pour tout $j \in \{1, \cdots, k\}$, on dispose de $\sigma_j \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $a_j = \sigma_j(a)$ (d'après la remarque 5.1.8. de [Galois]). Puis, d'après la proposition 6.2.1. de [Galois], $\mathrm{Gal}(K/\mathbb{Q})$ agit par élévation des racines de l'unité à une puissance inversible dans $\mathbb{Z}/N\mathbb{Z}$. Donc pour tout $j \in \{1, \cdots, k\}$, on dispose de $m_j \in \mathbb{Z}$ premier avec N tel que $\sigma_j(e^{\frac{2i\pi}{N}}) = e^{\frac{2im_j\pi}{N}}$. Ainsi :

$$\forall j \in \{1, \cdots, k\}, \quad a_j = \sigma_j(a) = \frac{1}{n}\sum_{i=1}^n \sigma_j(\lambda_i) = \frac{1}{n}\sum_{i=1}^n \lambda_i^{m_j}$$

Ainsi, $|a_j| \leq 1$. Considérons $b := \prod_{j=1}^k a_j$. Alors $|b| \leq 1$, d'après ce qui précède, et $b \in \mathbb{Q}$ car c'est (au signe près), le coefficient constant du polynôme minimal de a sur $\mathbb{Q}$.

Supposons maintenant que a soit entier algébrique. Alors il en est de même pour tous les conjugués de a (le polynôme minimal de a divisant tout polynôme annulateur de a). Ainsi, b est entier algébrique comme produit d'entiers algébriques. Comme $b \in \mathbb{Q}$, il s'ensuit que $b \in \mathbb{Z}$ et puisque $|b| \leq 1$ on a $b \in \{-1, 0, 1\}$. Si $a \neq 0$, alors aucun des conjugués de a n'est nul (car 0 est le seul conjugué de 0) donc $b \neq 0$ et ainsi $|b| = 1$. Il s'ensuit que $|a| = 1$. Il y a donc égalité dans l'inégalité triangluaire donc les λ_i sont positivement liés, et comme ils sont tous de module 1, ils sont tous égaux. □

Proposition 3.2.2. *Soit (V, ρ) une représentation linéaire complexe irréductible d'un groupe fini G. Soit $g \in G$ et $C_G(g)$ la classe de conjugaison de G dans G. Si $|C_G(g)|$ est premier avec $\dim(V)$ et si $\chi_\rho(g) \neq 0$ alors $\rho(g)$ est une homothétie.*

Démonstration. Comme $|C_G(g)| \wedge \dim(V) = 1$, le théorème de Bézout assure l'existence de $(a, b) \in \mathbb{Z}^2$ tel que $a|C_G(g)| + b\dim(V) = 1$. On a alors :

$$\frac{\chi_\rho(g)}{\dim(V)} = \frac{(a|C_G(g)| + b\dim(V))\chi_\rho(g)}{\dim(V)} = a\frac{|C_G(g)|}{\dim(V)}\chi_\rho(g) + b\chi_\rho(g)$$

Or, $\chi_\rho(g)$ est entier algébrique (comme somme de racines de l'unité qui sont des nombres algébriques) et $\frac{|C_G(g)|}{\dim(V)}\chi_\rho(g)$ est algébrique d'après le théorème 1.7.1 donc $\frac{\chi_\rho(g)}{\dim(V)}$ est algébrique. Posons $n := \dim(V)$ et notons $\lambda_1, \cdots, \lambda_n$ les valeurs propres de $\rho(g)$ (qui sont des racines de l'unité). Alors :

$$\frac{\chi_\rho(g)}{\dim(V)} = \frac{1}{n}\sum_{i=1}^n \lambda_i$$

Comme $\chi_\rho(g) \neq 0$, le lemme précédent assure que $\lambda_1 = \cdots = \lambda_n$ donc que $\rho(g)$ est une homothétie. □

Proposition 3.2.3. *Soit G un groupe fini et $g \in G \setminus \{1\}$ tel que $|C_G(g)| = p^\alpha$ avec p premier et $\alpha \in \mathbb{N}^*$. Alors il existe un sous-groupe distingué $H \subsetneq G$ tel que $\overline{g}$, la classe de G modulo H soit dans $Z(G/H)$.*

Démonstration. On va prendre $H = \ker(\chi_\rho) = \ker(\rho)$ pour une certaine représentation (V, ρ). H sera alors un sous-groupe distingué de G d'après le point (iv) de la proposition 1.3.4. Pour que $H \subsetneq G$, il s'agira de vérifier que $\chi_\rho \neq 1$. Notons aussi que ρ induit une bijection entre G/H et $\rho(G)$. Pour que $\overline{g} \in Z(G/H)$, il suffit donc de montrer que $\rho(g) \in Z(\rho(G))$. C'est en particulier le cas si $\rho(g)$ est une homothétie.

D'où l'idée d'appliquer le lemme précédent. Il s'agit de trouver $\chi \in \mathrm{Irr}(G) \setminus \{1\}$ tel que $\chi(g) \neq 0$ et $p \nmid \chi(1) = \dim(W_\chi)$. Supposons par l'absurde qu'un tel caractère n'existe pas, c'est à dire que pour tout $\chi \in \mathrm{Irr}(G) \setminus \{1\}$, $\chi(g) = 0$ ou $p|\chi(1)$. Soit χ_G le caractère associé à la représentation régulière de G. Alors d'après le point (i) du corollaire 1.5.9 :

$$\chi_G = \sum_{\chi \in \mathrm{Irr}(G)} \dim(W_\chi)\chi = 1 + \sum_{\chi \in \mathrm{Irr}(G)\setminus\{1\}} \chi(1)\chi$$

Comme $\chi_G(h) = |G|\delta_{h,1}$ pour tout $h \in G$, on obtient alors en évaluant l'égalité ci-dessous en $g \in G \setminus \{1\}$:

$$1 + \sum_{\chi \in \mathrm{Irr}(G)\setminus\{1\}} \chi(1)\chi(g) = 0$$

Ainsi :

$$\frac{1}{p} = -\sum_{\chi \in \mathrm{Irr}(G)\setminus\{1\}} \frac{\chi(1)\chi(g)}{p}$$

Comme pour tout $\chi \in \mathrm{Irr}(G) \setminus \{1\}$, $\chi(g)$ est entier algébrique et que $\chi(g) = 0$ dès que $p \nmid \chi(1)$, il s'ensuit que $\frac{1}{p}$ est algébrique comme combinaison linéaire entière d'entiers algébriques. Or, $\frac{1}{p} \in \mathbb{Q}$. Donc $\frac{1}{p}$ est entier. C'est absurde ! D'où le résultat. □

On peut alors, comme le suggérait la discussion du paragraphe précédent, achever la preuve du :

Théorème 3.2.4 (Burnside, 1905)**.** *Tout groupe de cardinal admettant au plus deux facteurs premiers est résoluble.*

Démonstration. On le prouve par récurrence sur le cardinal du groupe.

L'initialisation est triviale car un groupe trivial est résoluble.

Soient p, q des nombres premiers et $\alpha, \beta \in \mathbb{N}^*$. Supposons le résultat vrai pour tous les groupes de cardinal divisant strictement $p^\alpha q^\beta$ et soit G un groupe de cardinal $p^\alpha q^\beta$. Si $Z(G)$ est non trivial, on peut appliquer l'hypothèse de récurrence à $G/Z(G)$ et conclure grâce à la proposition 1.3.4.

Supposons donc que $Z(G) = \{1\}$. Comme nous l'avons vu à la fin du paragraphe précédent, l'équation aux classes :

$$p^\alpha q^\beta = |G| = 1 + \sum_{i=1}^{k} |C_G(g_i)| = 1 + \sum_{i=1}^{k} \frac{|G|}{|G_{g_i}|}$$

assure l'existence de $g \in G \setminus \{1\}$ tel que $|C_G(g)| = p^\gamma$ avec $\gamma \in \mathbb{N}$. On applique alors la proposition précédente qui assure l'existence d'un sous-groupe $H \subsetneq G$ distingué dans G tel que $\overline{g} \in Z(G/H)$. Mais alors H n'est pas trivial car sinon on aurait $g \in Z(G)$ donc $g = 1$ puisque $Z(G)$ est trivial par hypothèse. On applique donc l'hypothèse de récurrence à H et G/H ainsi que la proposition 1.3.4. D'où l'itération et le théorème. □

4 Une troisième application de la théorie des caractères : le théorème de Suzuki.

Pour continuer dans l'étude de la résolubilité ds groupes, nous prouvons un cas particulier du théorème de Feit-Thomson dont la preuve est bien trop longue et difficile pour être comprise à notre niveau.

Théorème 4.0.1 (Feit-Thompson)**.** *Tout groupe fini d'ordre impair est résoluble.*

Suzuki prouve ce résultat pour les groupes d'ordre impair ayant en outre la propriété d'être *commutant abélien*, que l'on abrègera en CA.

4.1 Groupes CA et résolubilité.

Définition 4.1.1. *On dit qu'un groupe G est* commutant abélien *ou CA lorsque pour tout $g \in G \setminus \{1\}$ le centralisateur de g, $Z(g) = \{h \in G | hg = gh\}$ est abélien.*

Remarque 4.1.2. Un groupe fini G est CA si et seulement si la relation binaire de commutation sur $G \setminus \{1\}$ est une relation d'équivalence (le point non trivial étant la transitivité).

Exemple 4.1.3. Tout groupe abélien est trivialement CA. $GA(\mathbb{F}_q)$ est aussi un groupe CA (non-abélien). En effet, si $g : x \longmapsto ax + b$ est un élément de $GA(\mathbb{F}_q) \setminus \{\mathrm{id}_{\mathbb{F}_q}\}$ et si $h : x \longmapsto cx + d$ et $h' : x \longmapsto c'x + d'$ sont dans $Z(g)$ alors on a :

$$\forall x \in \mathbb{F}_q, \quad a(cx+d)+b = c(ax+b)+d \quad \text{ie} \quad acx+ad+b = acx+bc+d \quad \text{ie} \quad ad+b = bc+d$$

De même $ad' + b = bc' + d'$. Il s'agit de vérifier que $cd' + d = c'd + d'$. Si $b \neq 0$ alors on a :

$$b(cd'+d) = bcd'+bd = (ad+b-d)d'+bd = (ad'+b)d+(b-d)d' = (bc'+d')d+(b-d)d' = b(c'd+d')$$

et donc $cd' + d = c'd + d'$ en simplifiant. Sinon, $a \neq 0$ (car $g \neq \mathrm{id}_{\mathbb{F}_q}$) et alors $ad = d$ et $ad' = d'$ donc $d = d' = 0$ donc trivialement $cd' + d = c'd + d'$. Donc $hh' = h'h$ et $GA(\mathbb{F}_q)$ est bien CA.

Exemple 4.1.4. Lorsque q est une puissance de 2, $SL_2(\mathbb{F}_q)$ est un groupe CA. Le prouver est loin d'être trivial, aussi invitons-nous le lecteur à se reporter à l'annexe B pour plus de détails.

Nous allons montrer que la propriété de commutant abélien est très commode pour raisonner par récurrence. En effet, on a la :

Proposition 4.1.5. *Soit G un groupe CA d'ordre impair non-abélien et non-simple (donc admettant un sous-groupe distingué propre). Supposons tous les groupes CA d'ordre impair inférieur à $|G|$ résolubles. Alors G est résoluble.*

Démonstration. Pour commencer, on sait que G admet un sous-groupe distingué propre H qui est CA car G est CA donc résoluble par hypothèse. D'après la proposition 3.0.2, il suffirait de montrer que G/H est résoluble pour conclure. C'est en particulier le cas si G/H est CA.

Il s'agirait donc de vérifier que si $a, b, c \in G \setminus H$, sont tels que a et b d'une part et b et c d'autre part commutent modulo H alors a et c commutent modulo H. Remarquons que ceci équivaut à $b^{-1}a^{-1}ba \in H$ et $c^{-1}b^{-1}cb \in H$. En particulier $bah = ab$ et $bch' = cb$ pour $h, h' \in H$: ce sont "presque" des relations de commutation dans G. Si l'on parvenait "en forçant un peu" à en faire des relations de commutation dans G par exemple du type $bak = akb$ et $bck' = ck'b$ avec $k, k' \in H$ alors on aurait $ak, ck' \in Z(b)$ et donc $akck' = ck'ak$ car $b \neq 1$ et que G est CA. Ainsi :

$$akck' = ac(c^{-1}kc)k' = ck'ak = ca(a^{-1}k'a)k$$

Et donc :

$$ac = ca(a^{-1}k'a)kk'^{-1}(c^{-1}kc)^{-1}$$

avec $(a^{-1}k'a)kk'^{-1}(c^{-1}kc)^{-1} \in H$ car H est distingué et ainsi a et c commutent modulo H.

Il s'agit donc de transformer les relations de commutation comme indiqué précédemment. Remarquons que si l'on écrit $b^{-1}a^{-1}ba = b^{-1}kbk^{-1}$ pour $k \in H$, alors on obtient $bak = akb$ comme voulu. Il s'agit donc de savoir si l'on peut écrire tout élément de H sous la forme $b^{-1}kbk^{-1}$. Il faudrait donc que $\phi : h \in H \longmapsto b^{-1}hbh^{-1} \in H$ soit surjective, donc bijective puisque H est fini. Si c'était un morphisme de groupes, il suffirait de vérifier que son noyau est trivial (ce qui est plus simple à vérifier en général). Or, ϕ est un morphisme de groupes lorsque H est abélien. En effet, on a alors pour tout $h, h' \in H$ alors :

$$\begin{aligned} b^{-1}hh'b(hh')^{-1} &= b^{-1}hh'bh'^{-1}h^{-1} = b^{-1}hbh^{-1}h(b^{-1}h'b)h'^{-1}h^{-1} = b^{-1}hbh^{-1}(b^{-1}h'b)h'^{-1}h^{-1}h \\ &= (b^{-1}hbh^{-1})(b^{-1}h'bh'^{-1}) \end{aligned}$$

Supposons donc H abélien. Alors pour $h \in H$, $\phi(h) = 1$ donne $b \in Z(h)$. Or, $H \subset Z(h)$ car H est abélien. Comme $b \notin H$, il suffirait que $Z(h) = H$ pour tout $h \in H \setminus \{1\}$ pour que ϕ soit injective. C'est en particulier le cas si H est un sous-groupe abélien maximal.

En général, tout sous-groupe distingué propre de G n'est pas abélien maximal. Il s'agit donc de montrer l'existence d'un tel sous-groupe H. Soit N un sous-groupe distingué propre de G. Alors comme G est CA, N est CA donc résoluble. Donc la suite des groupes dérivés de N, $(D^n(N))_{n\in\mathbb{N}}$ [4] stationne au groupe trivial à partir d'un certain rang $n_0 \in \mathbb{N}^*$. On sait qu'alors $D^{n_0-1}(N)$ est un groupe abélien non trivial. En outre, pour tout $g \in G$, $k \in N \longmapsto gkg^{-1}$ est un automorphisme de N (puisque N est distingué), donc il stabilise la suite des sous-groupes dérivés de N (l'image d'un commutateur par un morphisme de groupes étant un commutateur) donc en particulier $D^{n_0-1}(N)$ est distingué dans G. Prenons pour H le commutant de $D^{n_0-1}(N)$. On sait qu'alors H est abélien car c'est une intersection de commutants d'éléments non-triviaux et que G est CA. En outre, si $h \in H$ alors pour tout $k \in D^{n_0-1}(N)$, et tout $g \in G$, $g^{-1}kg \in D^{n_0-1}(N)$ donc comme $D^{n_0-1}(N)$ est abélien :

$$kghg^{-1} = g(g^{-1}kg)hg^{-1} = gh(g^{-1}kg)g^{-1} = ghg^{-1}k$$

donc $ghg^{-1} \in H$. Ainsi, H est distingué dans G. Enfin, si $H \subset H'$ avec H' abélien, on a pour tout $k \in D^{n_0-1}(N)$, $H' \subset Z(k)$ puisque $D^{n_0-1}(N) \subset H$ donc :

$$H' \subset \bigcap_{k\in D^{n_0-1}(N)} Z(k) = H$$

Donc H est bien abélien maximal. Ceci conclut la preuve de la proposition d'après la discussion ci-dessus. □

Pour qu'une récurrence permette de conclure, il suffit donc de prouver qu'aucun groupe CA non-abélien d'ordre impair est simple.

4.2 Une stratégie de preuve.

Dans toute la suite, on fixe donc G un groupe d'ordre impair que l'on suppose non-abélien, CA et simple. Il s'agit de montrer qu'un tel groupe n'existe pas, donc d'aboutir à une contradiction.

Pour commencer, nous allons obtenir une partition de G semblable à la partition de Frobenius obtenue au lemme 2.1.7.

Remarquons que pour tout $g \in G$, $Z(g) := \{h \in G | gh = hg\}$ est un sous-groupe abélien maximal de G contenant g. Donc G est recouvert par des sous-groupes abéliens maximaux.

4. Où pour tout groupe K quelconque $D(K)$ désigne le sous-groupe de K engendré par les commutateurs de K.

Lemme 4.2.1. *Les sous-groupes abéliens maximaux de G ne s'intersectent qu'en l'élément neutre.*

Démonstration. En effet, si H et H' sont des sous-groupes abéliens maximaux de G tels que $H \cap H' \neq \{1\}$, alors on prend $h_0 \in H \cap H' \neq \{1\}$, de sorte que tous $h \in H$ et $h' \in H'$ commutent avec h_0 donc commutent entre eux car G est CA et que $h_0 \neq 1$. Ainsi, le sous-groupe engendré par H et H' est un groupe abélien qui contient H et H' donc qui égalise H et H' par maximalité. Donc $H = H'$. □

Les $H \setminus \{1\}$ avec H sous-groupe abélien maximal de G forment donc une partition de $G \setminus \{1\}$.

En outre, si H est un sous-groupe abélien maximal de G, alors il en est de même pour gHg^{-1} pour tout $g \in G$. Ainsi, G agit par conjugaison sur l'ensemble de ses sous-groupe abéliens maximaux. Soit $\{H_1, \cdots, H_n\}$ un système de représentants des orbites sous une telle action. Alors les $gH_ig^{-1} \setminus \{1\}$ pour $i \in \{1, \cdots, n\}$ et $g \in G$ forment une partition de G. De plus, pour $i \in \{1, \cdots, n\}$, $g, g' \in G$ fixés, $gH_ig^{-1} = g'H_ig'^{-1}$ équivaut à g et g' congrus modulo $N(H_i) := \{h \in G | hH_ih^{-1} = H_i\}$. On peut donc poser $\overline{g}H_i\overline{g}^{-1} := gH_ig^{-1}$ pour tout représentant g de $\overline{g} \in G/N(H_i)$ en remarquant que les $\overline{g}H_i\overline{g}^{-1} \setminus \{1\}$ sont disjoints quand i parcourt $\{1, \cdots, n\}$ et $\overline{g}$ parcourt $G/N(H_i)$. On en déduit la :

Proposition 4.2.2. *On a :*

$$G = \{1\} \sqcup \bigsqcup_{i=1}^{n} \bigsqcup_{\overline{g} \in G/N(H_i)} \overline{g}H_i\overline{g}^{-1} \setminus \{1\}$$

ce qui donne en passant aux cardinaux et en divisant par $|G|$:

$$1 = \frac{1}{|G|} + \sum_{i=1}^{n} \left(\frac{1}{|W_i|} - \frac{1}{|H_i||W_i|} \right)$$

où pour tout $i \in \{1, \cdots, n\}$, $W_i := N(H_i)/H_i$ (c'est un groupe car H_i est distingué dans $N(H_i)$).

Exemple 4.2.3. Cette décomposition de G est inspirée de celle du groupe $SL_2(\mathbb{F}_q)$ lorsque q est une puissance de 2. La proposition B.0.1 assure que $SL_2(\mathbb{F}_q)$ est un groupe CA qui admet trois sous-groupes abéliens maximaux : le tore T_1, le groupe unipotent T_2 et le tore non-scindé T_3 donnés respectivement par :

$$T_1 := \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} | \lambda \in \mathbb{F}_q^* \right\}, \quad T_2 := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} | x \in \mathbb{F}_q \right\}$$

et

$$T_3 := \left\{ \begin{pmatrix} \alpha & \beta \\ \beta y & \alpha + \beta \end{pmatrix} | (\alpha, \beta) \in \mathbb{F}_q^2, \, \alpha^2 + \alpha\beta + \beta^2 y = 1 \right\}$$

où y est un élément de $\mathbb{F}_q$ qui n'est pas dans l'image de $x \in \mathbb{F}_q \longmapsto x^2 + x \in \mathbb{F}_q$. Les conjugués de ces groupes recouvrent de même $SL_2(\mathbb{F}_q)$ et on a la partition :

$$SL_2(\mathbb{F}_q) = \{I_2\} \sqcup \bigsqcup_{i=1}^{3} \bigsqcup_{\overline{P} \in SL_2(\mathbb{F}_q)/N(T_i)} \overline{P}T_i\overline{P}^{-1} \setminus \{I_2\}$$

On peut déjà remarquer que $\frac{1}{|G|} - \sum_{i=1}^{n} \frac{1}{|H_i||W_i|} \leq 0$ car $|H_1||W_1| = |N(H_1)| \leq |G|$. On a donc :

$$1 \leq \sum_{i=1}^{n} \frac{1}{|W_i|}$$

Il suffirait donc de trouver un majorant de $\sum_{i=1}^{n} \frac{1}{|W_i|}$ qui soit strictement inférieur à 1 pour aboutir à une contradiction. Cela revient à majorer n et à minorer au maximum les $|W_i|$. On peut déjà obtenir le résultat suivant :

Lemme 4.2.4. *Pour tout $i \in \{1, \cdots, n\}$, $|W_i| \geq 3$.*

Démonstration. Si par l'abusurde W_i était trivial pour $i \in \{1, \cdots, n\}$ fixé alors on aurait $N(H_i) = H_i$ et donc $gH_ig^{-1} \cap H_i = \{1\}$ pour tout $g \in G \setminus H_i$ (les sous-groupes abéliens maximaux étant d'intersection triviale d'après le lemme 4.2.1). Donc G est un groupe de Frobenius de complément de Frobenius H_i. Donc d'après le théorème de Frobenius (verson 1), on dispose d'un sous-groupe distingué K de G tel que $G = K \rtimes H_i$. Mais comme G est simple, on a alors $H_i = \{1\}$ et $K = G$ ou $H_i = G$ et $K = \{1\}$. Le premier cas est impossible car $N(\{1\}) = G \neq \{1\}$ et le deuxième cas aussi car G n'est pas abélien.

Donc W_i est non trivial pour tout $i \in \{1, \cdots, n\}$. Mais d'après le théorème de Lagrange, $|W_i|$ divise $|G|$ qui est impair, donc $|W_i|$ est impair. Ainsi, $|W_i| \geq 3$. □

Remarque 4.2.5. Combiné à l'inégalité $1 \leq \sum_{i=1}^{n} \frac{1}{|W_i|}$, le lemme précédent donne que $n \geq 3$.

4.3 Conclusion à l'aide de la théorie des caractères.

4.3.1 Caractères exceptionnels.

Soit H l'un des sous-groupes abéliens maximaux H_i de G (on omet la dépendance en i pour alléger les notations). Alors $N(H)$ agit sur H par conjugaison. En outre, si $g, g' \in N(H)$ sont congrus modulo H alors $g' = gh'$ pour $h' \in H$ et pour tout $h \in H$, $g'hg'^{-1} = gh'hh'^{-1}g^{-1} = ghg^{-1}$ puisque H est abélien. Ainsi, $W := N(H)/H$ agit aussi sur H par conjuguaison (les conjugués étant indépendants des représentants des classes modulo H). On définit ainsi une action de W sur $\mathrm{Irr}(H)$ en posant pour tous $\chi \in \mathrm{Irr}(H)$, $w \in W$ et $h \in H$:

$$w \cdot \chi(g) := \chi(wgw^{-1})$$

Lemme 4.3.1. **(i)** *Tout élément non trivial de W ne fixe aucun élément non trivial de $Irr(H)$ sous cette action.*

(ii) *Le nombre d'orbites de $Irr(H) \setminus \{1\}$ sous l'action de W est $\frac{|H|-1}{|W|} \geq 2$.*

Démonstration. **(i)** Commençons par vérifier que (i) est vrai pour l'action de W sur H. Soit $w \in W \setminus \{1\}$. Si par l'absurde w fixe un élément $h \in H \setminus \{1\}$ alors tout représentant g de w (qui n'est pas dans H puisque $w \neq 1$) commute avec h et donc le commutant de h contient H et $g \notin H$. Comme G est CA, ce commutant est abélien et ceci contredit la maximalité de H.

Supposons maintenant par l'absurde que w fixe $\chi \in \mathrm{Irr}(H) \setminus \{1\}$ alors $\chi(whw^{-1}) = \chi(h)$ pour tout $h \in H$. Or, vu que H est abélien, le corollaire 1.5.10 assure que χ est le caractère d'une représentation de dimension 1, donc que c'est un morphisme de groupes de G vers S^1. Ainsi, $\chi(whw^{-1}h^{-1}) = \chi(1) = 1$ pour tout $h \in H$.

Or, puisque H est abélien, $h \in H \longmapsto whw^{-1}h^{-1} \in H$ est un morphisme de groupes. Il est injectif puisque w ne fixe aucun élément non trivial de H donc surjectif. Ainsi, $\chi = 1$. Absurde ! Ceci prouve le premier point.

(ii) Ainsi, les orbites de tous les éléments non triviaux de $\mathrm{Irr}(H)$ ont $|W|$ éléments. Puisque ces orbites forment une partition de $\mathrm{Irr}(H) \setminus \{1\}$, il y en a donc $\frac{|\mathrm{Irr}(H)|-1}{|W|}$. Mais $|\mathrm{Irr}(H)|$ est le nombre de classes de conjugaisons de H d'après le corollaire 1.5.5. Comme H est abélien, on a donc $|\mathrm{Irr}(H)| = |H|$ donc il y a $\frac{|H|-1}{|W|}$ orbites. $|H|$ et $|W|$ étant impairs (puisque G est d'ordre impair) et H étant non trivial (car abélien maximal) cette quantité est nécessairement ≥ 2. □

Lemme 4.3.2. *Soient $\chi, \chi' \in Irr(H)$ appartenant à des orbites distinctes sous l'action de W. Alors le caractère généralisé $Ind_H^G\chi - Ind_H^G\chi'$ est la différence de deux caractères irréductibles de G.*

Démonstration. Comme dans la preuve du lemme 2.2.1, il s'agit de calculer la norme du caractère généralisé $\phi := \mathrm{Ind}_H^G\chi - \mathrm{Ind}_H^G\chi'$ et d'utiliser le lemme 1.5.11. On sait par le théorème 1.6.2 que :

$$\forall g \in G, \quad \phi(g) = \frac{1}{|H|} \sum_{\substack{s \in G \\ g \in s^{-1}Hs}} (\chi(sgs^{-1}) - \chi'(sgs^{-1}))$$

Puisque $\chi(1) = \chi'(1) = 1$, il est alors immédiat que ϕ est à support dans $\bigcup_{s\in G} s^{-1}Hs \setminus \{1\} = \bigsqcup_{\overline{g}\in G/N(H)} \overline{g}H\overline{g}^{-1} \setminus \{1\}$. En outre, si $h \in H \setminus \{1\}$ et $s \in G$ alors $h \in s^{-1}Hs \iff sH = Hs \iff s \in N(H)$ et de plus, pour tous $s, s' \in N(H)$, on a par maximalité de H que $H = Z(h)$ et donc :

$$shs^{-1} = s'hs'^{-1} \iff (s'^{-1}s)h(s'^{-1}s)^{-1} = h \iff s'^{-1}s \in Z(h) = H \iff s \text{ et } s' \text{ ont même classe dans } W$$

en partitionnant $N(H)$ en ses $\frac{|N(H)|}{|H|} = |W|$ classes modulo H, on obtient donc que :

$$\phi(h) = \sum_{w\in W} (\chi(whw^{-1}) - \chi'(whw^{-1}))$$

Donc sur H, ϕ coïncide avec le caractère généralisé $\sum_{w\in W}(w\cdot\chi - w\cdot\chi')$. Or, les $w\cdot\chi$ et $w\cdot\chi'$ sont des caractères irréductibles de H deux à deux distincts puisque χ et χ' ne sont pas dans la même orbite modulo W. Comme les caractères irréductibles sont orthogonaux (d'après le théorème 1.5.3), il s'ensuit que :

$$\sum_{h\in H}\left|\sum_{w\in W}(w\cdot\chi(h) - w\cdot\chi'(h))\right|^2 = |H|\left\langle \sum_{w\in W}(w\cdot\chi - w\cdot\chi'), \sum_{w\in W}(w\cdot\chi - w\cdot\chi')\right\rangle_H = 2|W||H|$$

Ainsi, comme ϕ est une fonction centrale :

$$\begin{aligned}\langle\phi,\phi\rangle &= \frac{1}{|G|}\sum_{g\in G}|\phi(g)|^2 = \frac{1}{|G|}\sum_{\overline{g}\in G/N(H)}\sum_{h\in\overline{g}H\overline{g}^{-1}\setminus\{1\}}|\phi(h)|^2 = \frac{1}{|G|}\frac{|G|}{|N(H)|}\sum_{h\in H\setminus\{1\}}|\phi(h)|^2 \\ &= \frac{1}{|N(H)|}\sum_{h\in H}\left|\sum_{w\in W}(w\cdot\chi(h) - w\cdot\chi'(h))\right|^2 = \frac{2|W||H|}{|N(H)|} = 2\end{aligned}$$

Le lemme 1.5.11 donne alors immédiatement que ϕ est la somme ou la différence de deux caractères irréductibles de G. Puisque $\phi(1) = 0$, c'est nécessairement une différence. □

Proposition 4.3.3 (Caractères exceptionnels)**.** *Notons $m := \frac{|H|-1}{|W|}$ le nombre d'orbites de $Irr(H)\setminus\{1\}$ sous l'action de W et considérons $\chi_1, \cdots, \chi_m$, un système de représentants de ces orbites. Alors il existe m caractères irréductibles de G distincts : $\chi_1^*, \cdots, \chi_m^*$ et un signe $\epsilon \in \{\pm 1\}$ tels que :*

$$\forall 1 \le k \ne l \le m, \quad Ind_H^G\chi_k - Ind_H^G\chi_l = \epsilon(\chi_k^* - \chi_l^*)$$

Pour $m \ge 3$, cette écriture est unique et pour $m = 2$, elle est unique à échange près de χ_1^* et χ_2^* (en changeant ϵ en $-\epsilon$). On appelle caractères exceptionnels de H *les caractères χ_k^*.*

Démonstration. Pour $m = 2$, l'existence est une conséquence immédiate du lemme précédent. "L'unicité" est claire puisque les caractères irréductibles forment une base des fonctions centrales (d'après le théorème 1.5.3).

Supposons $m \ge 3$. Le lemme précédent assure l'existence d'une famille $(\chi_{k,l}^*)_{1\le k\ne l\le m}$ de caractères irréductibles de G telle que :

$$\forall 1 \le k \ne l \le m, \quad \mathrm{Ind}_H^G\chi_k - \mathrm{Ind}_H^G\chi_l = \chi_{k,l}^* - \chi_{l,k}^*$$

la symétrie de la formule étant obtenue avec la relation triviale $\mathrm{Ind}_H^G\chi_k - \mathrm{Ind}_H^G\chi_l = -(\mathrm{Ind}_H^G\chi_l - \mathrm{Ind}_H^G\chi_k)$. La famille des $\chi_{k,l}^*$ est de plus unique d'après le théorème d'orthonormalité des carcatères.

Soient $1 \le k, k', l, l' \le m$ tous distincts. Alors :

$$\mathrm{Ind}_H^G\chi_k - \mathrm{Ind}_H^G\chi_l + \mathrm{Ind}_H^G\chi_{k'} - \mathrm{Ind}_H^G\chi_{l'} = \chi_{k,l}^* - \chi_{l,k}^* + \chi_{k',l'}^* - \chi_{l',k'}^*$$

Mais puisque k, k', l, l' sont tous distincts, les caractères de H associés sont dans des orbites distinctes

sous l'action de W et on obtient alors en vertu d'un calcul identique à celui du lemme précédent que le produit scalaire du membre de droite de cette équation avec lui-même est 4. Ainsi, nécessairement $\chi^*_{k,l}, \chi^*_{l,k}, \chi^*_{k',l'}$ et $\chi^*_{l',k'}$ sont tous distincts.

On cherche maintenant à établir des égalités entre les $\chi^*_{k,l}$. On sait que :

$$\mathrm{Ind}_H^G\chi_1 - \mathrm{Ind}_H^G\chi_2 = \chi^*_{1,2} - \chi^*_{2,1} \quad \text{et} \quad \mathrm{Ind}_H^G\chi_2 - \mathrm{Ind}_H^G\chi_3 = \chi^*_{2,3} - \chi^*_{3,2}$$

Donc par somme :

$$\chi^*_{1,3} - \chi^*_{3,1} = \mathrm{Ind}_H^G\chi_1 - \mathrm{Ind}_H^G\chi_3 = \chi^*_{1,2} - \chi^*_{2,1} + \chi^*_{2,3} - \chi^*_{3,2}$$

Donc par orthonormalité des caractères, l'une des deux série d'égalités suivantes est vérifiée :

$$\chi^*_{1,2} = \chi^*_{3,2} \quad \text{et} \quad \chi^*_{2,3} = \chi^*_{1,3} \quad \text{et} \quad \chi^*_{2,1} = \chi^*_{3,1} \quad (1)$$

Ou :

$$\chi^*_{2,1} = \chi^*_{2,3} \quad \text{et} \quad \chi^*_{1,2} = \chi^*_{1,3} \quad \text{et} \quad \chi^*_{3,2} = \chi^*_{3,1} \quad (2)$$

Supposons que (1) soit vérifié. Montrons alors par récurrence sur $k \in [\![\ 3\ ;\ m\ ]\!]$ que pour tout $b \in [\![\ 1\ ;\ k\ ]\!]$, la suite $(\chi^*_{a,b})_{1\leq a\neq b\leq k}$ est constante.

- Pour $k = 3$, on sait déjà que le résultat est vrai.
- Soit $k \in [\![\ 3\ ;\ m-1\ ]\!]$. Supposons le résultat au rang k. Soient $a, a' \in [\![\ 1\ ;\ k\ ]\!]$ distincts. Alors :

  $$\mathrm{Ind}_H^G\chi_a - \mathrm{Ind}_H^G\chi_{k+1} = \chi^*_{a,k+1} - \chi^*_{k+1,a} \quad \text{et} \quad \mathrm{Ind}_H^G\chi_{a'} - \mathrm{Ind}_H^G\chi_{k+1} = \chi^*_{a',k+1} - \chi^*_{k+1,a'}$$

  Ainsi, par différence :

  $$\chi^*_{a,a'} - \chi_{a',a} = \mathrm{Ind}_H^H\chi_a - \mathrm{Ind}_H^G\chi_{a'} = \chi^*_{a,k+1} - \chi^*_{k+1,a} - \chi^*_{a',k+1} + \chi^*_{k+1,a'}$$

  Il s'agit de montrer que $\chi^*_{a,k+1} = \chi^*_{a',k+1}$. On aura alors $\chi^*_{k+1,a} = \chi^*_{a',a}$ et $\chi^*_{k+1,a'} = \chi^*_{a,a'}$ et l'itération sera terminée.

  Supposons par l'absurde que $\chi^*_{a,k+1} \neq \chi^*_{a',k+1}$. Alors par orthogonalité des caractères, $\chi^*_{k+1,a} = \chi^*_{k+1,a'}$, $\chi_{a,a'} = \chi^*_{a,k+1}$ et $\chi_{a',a} = \chi_{a',k+1}$. Soit $b \in [\![\ 1\ ;\ k\ ]\!] \setminus \{a, a'\}$. On a alors $\chi^*_{b,a} = \chi^*_{a',a} = \chi_{a',k+1}$ et donc :

  $$\mathrm{Ind}_H^G\chi_b - \mathrm{Ind}_H^G\chi_a = \chi^*_{b,a} - \chi^*_{a,b} = \chi_{a',k+1} - \chi_{a,b}$$

  Puis :

  $$\mathrm{Ind}_H^G\chi_a - \mathrm{Ind}_H^G\chi_{k+1} = \chi^*_{a,k+1} - \chi^*_{k+1,a} = \chi^*_{a,k+1} - \chi^*_{k+1,a'}$$

  Donc par somme :

  $$\mathrm{Ind}_H^G\chi_b - \mathrm{Ind}_H^G\chi_{k+1} = \chi_{a',k+1} - \chi_{a,b} + \chi^*_{a,k+1} - \chi^*_{k+1,a'}$$

  Comme le produit scalaire du membre de gauche avec lui-même vaut 2 et que $\chi_{a',k+1} \neq \chi^*_{k+1,a'}$ (car $\mathrm{Ind}_H^G\chi'_a - \mathrm{Ind}_H^G\chi_{k+1} \neq 0$), on obtient que $\chi^*_{a,k+1} = \chi_{a,b}$. On montre de la même manière que $\chi^*_{a',k+1} = \chi_{a',b}$. Or, $\chi_{a,b} = \chi_{a',b}$ par hypothèse de récurrence. Donc $\chi^*_{a,k+1} = \chi^*_{a',k+1}$, ce qui contredit l'hypothèse de départ. D'où l'itération et le résultat.

Nous venons donc de montrer que $(\chi^*_{k,l})_{1\leq k\neq l\leq m}$ est constante pour tout $l \in [\![\ 1\ ;\ m\ ]\!]$. On peut donc poser $\chi^*_l := \chi^*_{k,l}$ pour tous $1 \leq k \neq l \leq m$, on obtient donc :

$$\forall 1 \leq k \neq l \leq m, \quad \mathrm{Ind}_H^G\chi_k - \mathrm{Ind}_H^G\chi_l = \chi^*_l - \chi^*_k = -(\chi^*_k - \chi^*_l)$$

Donc $\epsilon = -1$ convient. Dans le cas où (2) est vérifié, on montre avec une récurrence analogue que $(\chi^*_{k,l})_{1\leq k\neq l\leq m}$ est constante pour tout $k \in [\![1 ; m]\!]$ et on obtient le même résultat avec $\epsilon = 1$.

L'unicité de l'écriture obtenue est une conséquence triviale de l'orthogonalité des caractères irréductibles de G. □

Lemme 4.3.4. *Le caractère trivial n'est pas un caractère exceptionnel de H.*

Démonstration. Pour le montrer, il suffit de vérifier que pour tous $1 \leq k \neq l \leq m$, le coefficient de Fourier $\langle \mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l, 1\rangle$ est nul. Soient $1 \leq k \neq l \leq m$. Alors comme $\mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l$ est à support dans $\bigsqcup_{\overline{g}\in G/N(H)} \overline{g}H\overline{g}^{-1} \setminus \{1\}$ et que $\mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l$ est une fonction centrale, on obtient que :

$$\begin{aligned}\langle \mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l, 1\rangle &= \frac{1}{|G|} \sum_{\overline{g}\in G/N(H_i)} \sum_{h\in H} (\mathrm{Ind}_H^G \chi_k(h) - \mathrm{Ind}_H^G \chi_l(h)) \\ &= \frac{1}{|N(H)|} \sum_{h\in H} \sum_{w\in W} (\chi_k(whw^{-1}) - \chi_l(whw^{-1})) \\ &= \frac{|H|}{|N(H)|} \left\langle \sum_{w\in W} (w\cdot\chi_k - w\cdot\chi_l), 1 \right\rangle_H\end{aligned}$$

Et cette dernière quantité est nulle car 1 n'est dans l'orbite d'aucun des caractères irréductibles non-triviaux de H sous l'action de W. D'où le résultat. □

Lemme 4.3.5. *Les caractères exceptionnels de H sont tous égaux et entiers sur $G \setminus \bigsqcup_{\overline{g}\in G/N(H)} (\overline{g}H\overline{g}^{-1} \setminus \{1\})$.*

Démonstration. Si $\chi \in \mathrm{Irr}(H)$ et si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, alors χ^σ est le caractère d'une représentation de dimension 1 d'après le lemme 1.7.3 donc $\chi^\sigma \in \mathrm{Irr}(H)$. En outre, σ étant injectif, si $\chi \neq 1$ alors $\chi^\sigma \neq 1$. Donc $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur $\mathrm{Irr}(H) \setminus \{1\}$ et toujours par injectivité, si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, alors $\chi_1^\sigma, \cdots, \chi_m^\sigma$ est un système de représentants des classes de $\mathrm{Irr}(H) \setminus \{1\}$ sous l'action de W. Mais la proposition précédente assure que pour tous $1 \leq k \neq l \leq m$:

$$\mathrm{Ind}_H^G \chi_k^\sigma - \mathrm{Ind}_H^G \chi_l^\sigma = \epsilon(\chi_k^{*\sigma} - \chi_l^{*\sigma})$$

Or nous avons vu dans la preuve du lemme 4.3.2 (avec la formule du théorème 1.6.2) que les $\mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l$ ne dépendent pas des représentants χ_k et χ_l choisis mais seulement de leur classe sous l'action de W. Ainsi, les $\chi_k^{*\sigma}$ sont des caractères exceptionnels de H et on en déduit que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur les caractères exceptionnels de H.

Or, on a vu dans la preuve du lemme 4.3.2 que les $\mathrm{Ind}_H^G \chi_k - \mathrm{Ind}_H^G \chi_l$ sont nuls sur $G \setminus \bigsqcup_{\overline{g}\in G/N(H)} (\overline{g}H\overline{g}^{-1} \setminus \{1\})$. Ainsi, les caractères exceptionnels de H sont tous égaux sur $G \setminus \bigsqcup_{\overline{g}\in G/N(H)} (\overline{g}H\overline{g}^{-1} \setminus \{1\})$ donc $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixe $\chi_i^*(g)$, de sorte que $\chi_i^*(g) \in \mathbb{Q}$, pour tous $i \in [\![1 ; m]\!]$ et $g \in G \setminus \bigsqcup_{\overline{g}\in G/N(H)} (\overline{g}H\overline{g}^{-1} \setminus \{1\})$. Comme les valeurs prises par les caractères sont des entiers algèbriques, on a en fait $\chi_i^*(g) \in \mathbb{Z}$, pour tous $i \in [\![1 ; m]\!]$ et $g \in G \setminus \bigsqcup_{\overline{g}\in G/N(H)} (\overline{g}H\overline{g}^{-1} \setminus \{1\})$. □

Nous allons maintenant considérer tous les caractères irréductibles de G lorsque $H := H_i$ varie (pour $i \in [\![1 ; n]\!]$). On posera donc pour tout $i \in [\![1 ; n]\!]$, $m_i := \frac{|H_i|-1}{|W_i|}$, on notera $\chi_{i,1}, \cdots, \chi_{i,m_i}$ un système de représentants des classes de caractères irréductibles non triviaux de H_i sous l'action de W_i et $\chi^*_{i,1}, \cdots, \chi^*_{i,m_i}$ les caractères exceptionnels associés.

Proposition 4.3.6. *Tout caractère irréductible non-trivial de G est caractère exceptionnel de H_i pour un unique $i \in [\![1 ; n]\!]$.*

Démonstration. Soient $i, j \in [\![1 ; n]\!]$ distincts. Alors si $1 \leq k \neq l \leq m_i$ et $1 \leq k' \neq l' \leq m_j$, $\chi^*_{i,k} - \chi^*_{i,l}$ est à support dans $\bigsqcup_{\overline{g}\in G/N(H_i)} \overline{g}H_i\overline{g}^{-1} \setminus \{1\}$ et $\chi^*_{j,k'} - \chi^*_{j,l'}$ est à support dans $\bigsqcup_{\overline{g}\in G/N(H_j)} \overline{g}H_j\overline{g}^{-1} \setminus \{1\}$.

Ces deux supports étant disjoints, on en déduit que :

$$\langle \chi^*_{i,k} - \chi^*_{i,l}, \chi^*_{j,k'} - \chi^*_{j,l'} \rangle = \frac{1}{|G|} \sum_{g \in G} (\chi^*_{i,k}(g) - \chi^*_{i,l}(g))(\overline{\chi^*_{j,k'}(g)} - \overline{\chi^*_{j,l'}(g)}) = 0$$

Ainsi :

$$\langle \chi^*_{i,k}, \chi^*_{j,k'} \rangle - \langle \chi^*_{i,k}, \chi^*_{j,l'} \rangle - \langle \chi^*_{i,l}, \chi^*_{j,k'} \rangle + \langle \chi^*_{i,l}, \chi^*_{j,l'} \rangle = 0$$

Chacun des termes valant 0 ou 1 selon que les caractères dont on prend le produit scalaire sont égaux ou non. Supposons par l'absurde que $\chi^*_{i,k} = \chi^*_{j,k'}$. Alors $\langle \chi^*_{i,k}, \chi^*_{j,k'} \rangle = 1$ et donc $\langle \chi^*_{i,k}, \chi^*_{j,l'} \rangle = 1$ ou $\langle \chi^*_{i,l}, \chi^*_{j,k'} \rangle = 1$ i.e. $\chi^*_{i,k} = \chi^*_{j,l'}$ ou $\chi^*_{i,l} = \chi^*_{j,k'}$. Mais alors $\chi^*_{j,k'} = \chi^*_{j,l'}$ ou $\chi^*_{i,l} = \chi^*_{i,k}$, ce qui est exclus. Nous venons donc de voir que les familles $(\chi^*_{i,k})_{1 \leq k \leq m_i}$ et $(\chi^*_{j,k})_{1 \leq k \leq m_j}$ ne s'intersectent pas. Il y a donc au total $\sum_{i=1}^n m_i$ caractères irréductibles de G qui sont exceptionnels pour un H_i.

En outre, il est aisé de voir que pour tout $i \in [\![1 ; n]\!]$, $\bigsqcup_{\overline{g} \in G/N(H_i)} \overline{g} H_i \overline{g}^{-1} \setminus \{1\}$ contient m_i classes de conjugaisons de G (une par classe de conjugaison de $H \setminus \{1\}$ sous l'action de $W_i = N(H_i)/H_i$). Ainsi, la partition de la proposition 4.2.2 assure que $|\mathrm{Conj}(G)| = 1 + \sum_{i=1}^n m_i$. Le corollaire 1.5.5, assure qu'il y a donc $\sum_{i=1}^n m_i$ caractères irréductibles non triviaux de G, soit autant que de caractères exceptionnels. Or, d'après le lemme 4.3.4, tous les caractères exceptionnels sont non triviaux. D'où le résultat. □

4.3.2 Décomposition de Fourier de caractères généralisés particuliers.

Fixons $i \in [\![1 ; n]\!]$. Nous allons décomposer en série de Fourier le caractère généralisé :

$$\alpha_i := \mathrm{Ind}_{H_i}^G 1 - \mathrm{Ind}_{H_i}^G \chi_{i,1}$$

et ainsi obtenir des inégalités intéressantes sur les $|W_i|$ (au sens de la stratégie de preuve exposée au paragraphe 4.2) via l'étude des coefficients de Fourier obtenus.

Lemme 4.3.7. **(i)** *On a :* $\langle \alpha_i, \alpha_i \rangle = |W_i| + 1$

(ii) *Et la décomposition de Fourier de* α_i *s'écrit sous la forme :*

$$\alpha_i = 1 + a_i \sum_{k=1}^{m_i} \chi^*_{i,k} - \epsilon_i \chi^*_{i,1} + \sum_{1 \leq j \neq i \leq n} c_{i,j} \sum_{k=1}^{m_j} \chi^*_{j,k}$$

où a_i *et les* $c_{i,j}$ *sont des entiers.*

Démonstration. **(i)** D'après le théorème 1.6.2, on a :

$$\forall g \in G, \quad \alpha_i(g) = \frac{1}{|H_i|} \sum_{\substack{s \in G \\ g \in s^{-1} H_i s}} (1 - \chi_{i,1}(sgs^{-1}))$$

Il s'ensuit que α_i est à support dans $\bigsqcup_{\overline{g} \in G/N(H_i)} \overline{g} H_i \overline{g}^{-1} \setminus \{1\}$ et coincide avec $|W_i| - \sum_{w \in W_i} w \cdot \chi_{i,1}$ sur H_i. Le produit scalaire de ce caractère généralisé avec lui-même dans $L^2(H_i)$ étant égal à $|W_i|^2 + |W_i|$ et α_i étant une fonction centrale, on en déduit que :

$$\langle \alpha_i, \alpha_i \rangle = \frac{1}{|G|} \sum_{\overline{g} \in G/N(H_i)} \sum_{h \in \overline{g} H_i \overline{g}^{-1}} |\alpha_i(h)|^2 = \frac{1}{|N(H_i)|} \sum_{h \in H_i} |\alpha_i(h)|^2 = \frac{1}{|N(H_i)|} |H_i|(|W_i|^2 + |W_i|) = |W_i| + 1$$

(ii) $\chi_{i,1}$ étant distinct du caractère trivial, il en est de même pour $w \cdot \chi_{i,1}$ pour tout $w \in W_i$ (1 étant fixé sous l'action de W). Ainsi, par orthogonalité des caractères irréductibles, on a pour tout $w \in W_i$:

$$\sum_{h \in H_i} w \cdot \chi_{i,1}(h) = |H_i| \langle w \cdot \chi_{i,1}, 1 \rangle_H = 0$$

De sorte que :

$$\sum_{h\in H_i}\alpha_i(h)=\sum_{h\in H_i}\left(|W_i|-\sum_{w\in W_i}w\cdot\chi_{i,1}(h)\right)=|H_i||W_i|-\sum_{w\in W_i}\sum_{h\in H_i}w\cdot\chi_{i,1}(h)=|H_i||W_i|$$

Comme α_i est centrale et à support dans $\bigsqcup_{\overline{g}\in G/N(H_i)}\overline{g}H_i\overline{g}^{-1}\setminus\{1\}$, on en déduit que :

$$\langle\alpha_i,1\rangle=\frac{1}{|G|}\sum_{\overline{g}\in G/N(H_i)}\sum_{h\in\overline{g}H_i\overline{g}^{-1}}\alpha_i(h)=\frac{1}{|G|}\sum_{\overline{g}\in G/N(H_i)}\sum_{h\in H_i}\alpha_i(h)=\frac{1}{|G|}\frac{|G|}{|N(H_i)|}|H_i||W_i|=1$$

Soient $k,l\in[\![\,2\;;\;m_i\,]\!]$. Alors pour tous $w,w'\in W_i$, $w\cdot\chi_{i,1}$ est orthogonal à $w'\cdot\chi_{i,k}-w'\cdot\chi_{i,l}$, qui est aussi orthogonal à 1 (puisque les orbites sous l'action de W_i sont disjointes). Ainsi, pour tout $w'\in W_i$:

$$\begin{aligned}\sum_{h\in H_i}\alpha_i(h)(\overline{w'\cdot\chi_{i,k}(h)}-\overline{w'\cdot\chi_{i,l}(h)})&=|H_i||W_i|\langle 1,w'\cdot\chi_{i,k}-w'\cdot\chi_{i,l}\rangle_H\\&\quad-\sum_{w\in W_i}|H_i|\langle w\cdot\chi_{i,1},w'\cdot\chi_{i,k}-w'\cdot\chi_{i,l}\rangle_H=0\end{aligned}$$

Ainsi :

$$\begin{aligned}\langle\alpha_i,\chi_{i,k}^*-\chi_{i,l}^*\rangle&=\epsilon_i\langle\alpha_i,\mathrm{Ind}_{H_i}^G\chi_{i,k}-\mathrm{Ind}_{H_i}^G\chi_{i,l}\rangle\\&=\epsilon_i\frac{1}{|G|}\sum_{\overline{g}\in G/N(H_i)}\sum_{h\in\overline{g}H_i\overline{g}^{-1}}\alpha_i(h)\left(\overline{\mathrm{Ind}_{H_i}^G\chi_{i,k}(h)}-\overline{\mathrm{Ind}_{H_i}^G\chi_{i,l}(h)}\right)\\&=\epsilon_i\frac{1}{|G|}\frac{|G|}{|N(H_i)|}\sum_{h\in H_i}\alpha_i(h)\sum_{w\in W_i}(\overline{w\cdot\chi_{i,k}(h)}-\overline{w\cdot\chi_{i,l}(h)})\\&=\epsilon_i\frac{1}{|N(H_i)|}\sum_{w\in W_i}\sum_{h\in H_i}\alpha_i(h)(\overline{w\cdot\chi_{i,k}(h)}-\overline{w\cdot\chi_{i,l}(h)})=0\end{aligned}$$

Et donc les coefficients de Fourier $\langle\alpha_i,\chi_{i,k}^*\rangle$ pour $k\in[\![\,2\;;\;m_i\,]\!]$ sont tous égaux. On note a_i leur valeur commune.

Soit maintenant $k\in[\![\,2\;;\;m_i\,]\!]$. Pour tout $w'\in W_i$, $w'\cdot\chi_{i,1}$ est orthogonal à 1 et à tous les $w\cdot\chi_{i,1}$ pour $w\neq w'$ tandis que $w'\cdot\chi_{i,k}$ est orthogonal à tous les caractères cités sans exception. On en déduit que pour tout $w'\in W_i$:

$$\begin{aligned}\sum_{h\in H_i}\alpha_i(h)(\overline{w'\cdot\chi_{i,1}(h)}-\overline{w'\cdot\chi_{i,k}(h)})&=|W_i||H_i|\langle 1,w'\cdot\chi_{i,1}-w'\cdot\chi_{i,k}\rangle_H\\&\quad-\sum_{w\in W_i}|H_i|\langle w\chi_{i,1},w'\cdot\chi_{i,1}-w'\cdot\chi_{i,k}\rangle_H=-|H_i|\end{aligned}$$

Et donc qu'en vertu des calculs habituels :

$$\langle\alpha_i,\chi_{i,1}^*-\chi_{i,k}^*\rangle=\frac{-\epsilon_i|W_i||H_i|}{|N(H_i)|}=-\epsilon_i$$

Donc le coefficient de Fourier de α_i associé à $\chi_{i,1}^*$ est la somme $-\epsilon_i+a_i$.

Enfin, pour tous $j\in[\![\,1\;;\;n\,]\!]\setminus\{i\}$ et $k,l\in]\!]\,1\;;\;m_j\,]\!]$, $\chi_{j,k}^*-\chi_{j,l}^*$ est à support dans $\bigsqcup_{\overline{g}\in G/N(H_j)}\overline{g}H_j\overline{g}^{-1}\setminus\{1\}$, disjoint de $\bigsqcup_{\overline{g}\in G/N(H_i)}\overline{g}H_i\overline{g}^{-1}\setminus\{1\}$, le support de α_i donc :

$$\langle\alpha_i,\chi_{j,k}^*-\chi_{j,l}^*\rangle=0$$

Donc tous les coefficients de Fourier $\langle\alpha_i,\chi_{j,k}^*\rangle$ sont égaux à j fixé. Notons $c_{i,j}$ leur valeur commune.

Puisque tous les caractères irréductibles non triviaux de G sont exceptionnels (d'après la proposition 4.3.6), nous avons ainsi obtenu la décomposition de Fourier voulue. Bien-sûr, les coefficients de cette

décomposition de Fourier sont entiers puisque α_i est un caractère généralisé. □

Lemme 4.3.8. *On a :*

(i)
$$|\{j \in [\![1 \ ; \ n]\!] \setminus \{i\} \quad c_{i,j} \neq 0\}| \leq \frac{|W_i| - 1}{2}$$

(ii) *Et :*
$$\sum_{\substack{1 \leq j \neq i \leq n \\ c_{i,j}=0}} \left(\frac{1}{|W_j|} - \frac{1}{|W_j||H_j|} \right) \leq \frac{1}{m_i}$$

Démonstration. **(i)** En combinant les points (i) et (ii) du lemme précédent, on obtient que :

$$|W_i| + 1 = \langle \alpha_i, \alpha_i \rangle = 1 + (m_i - 1)a_i^2 + (a_i - \epsilon_i)^2 + \sum_{1 \leq j \neq i \leq n} c_{i,j}^2 m_j$$

Or, le point (ii) du lemme 4.3.1 assure que $m_i \geq 2$ donc si $a_i \neq 0$, $a_i^2 \geq 1$ car $a_i \in \mathbb{Z}$ et donc

$$(m_i - 1)a_i^2 + (a_i - \epsilon_i)^2 \geq m_i - 1 \geq 1$$

Puis, si $a_i = 0$, cette égalité est toujours vérifiée puisque $\epsilon_i \in \{\pm 1\}$. Donc :

$$\sum_{1 \leq j \neq i \leq n} c_{i,j}^2 m_j \leq |W_i| - 1$$

Comme $m_j \geq 2$ pour tout $1 \leq j \neq i \leq n$, d'après le point (ii) du lemme 4.3.1, et que les $c_{i,j}$ sont entiers, on obtient que :

$$|\{j \in [\![1 \ ; \ n]\!] \setminus \{i\} \quad c_{i,j} \neq 0\}| \leq \frac{1}{2} \sum_{1 \leq j \neq i \leq n} c_{i,j}^2 m_j \leq \frac{|W_i| - 1}{2}$$

(ii) Soit $j \in [\![1 \ ; \ n]\!] \setminus \{i\}$ tel que $c_{i,j} = 0$. Comme α_i est à support dans $\bigsqcup_{\overline{g} \in G/N(H_i)} \overline{g} H_i \overline{g}^{-1} \setminus \{1\}$, on a :

$$\forall g \in \bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}, \quad 0 = 1 + a_i \sum_{k=1}^{m_i} \chi_{i,k}^*(g) - \epsilon_i \chi_{i,1}^*(g) + \sum_{1 \leq j' \neq i, j \leq n} c_{i,j'} \sum_{k=1}^{m_{j'}} \chi_{j',k}^*(g) \quad (\star)$$

Or, si $1 \leq j' \neq j \leq n$, alors les $\chi_{j',k}^*$ sont des entiers tous égaux sur $\bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}$ (d'après le lemme 4.3.5) donc $\sum_{k=1}^{m_{j'}} \chi_{j',k}^*$ est un entier multiple de $m_{j'} = \frac{|H_{j'}|-1}{|W_{j'}|}$. Comme $|H_{j'}|$ et $|W_{j'}|$ sont impairs, il s'ensuit que $m_{j'}$ est pair donc que $\sum_{k=1}^{m_{j'}} \chi_{j',k}^*$ l'est aussi sur $\bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}$ et ce pour tout $1 \leq j' \neq j \leq n$. $(\star)$ assure alors que $\chi_{i,1}^*$ est impair sur $\bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}$. En, particulier $|\chi_{i,1}^*| \geq 1$ sur cet ensemble. Comme les caractères exceptionnels associés à H_i sont égaux sur $\bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}$ d'après le lemme 4.3.5, on obtient que :

$$\forall g \in \bigsqcup_{\overline{g} \in G/N(H_j)} \overline{g} H_j \overline{g}^{-1} \setminus \{1\}, \quad \left| \sum_{k=1}^{m_i} \chi_{i,k}^*(g) \right| \geq m_i$$

et ceci est vrai pour tout $j \in [\![1 \ ; \ n]\!] \setminus \{i\}$ tel que $c_{i,j} = 0$.

Ainsi, par orthogonalité des $\chi^*_{i,k}$, on obtient que :

$$\begin{aligned} m_i &= \left\langle \sum_{k=1}^{m_i} \chi^*_{i,k}, \sum_{k=1}^{m_i} \chi^*_{i,k} \right\rangle_G = \frac{1}{|G|} \sum_{g\in G} \left| \sum_{k=1}^{m_i} \chi^*_{i,k}(g) \right|^2 \\ &\geq \frac{1}{|G|} \sum_{\substack{1\leq j\neq i\leq n \\ c_{i,j}=0}} \sum_{g\in \bigsqcup_{\overline{g}\in G/N(H_j)} \overline{g}H_j\overline{g}^{-1}\setminus\{1\}} \left| \sum_{k=1}^{m_i} \chi^*_{i,1}(g) \right|^2 \geq \frac{1}{|G|} m_i^2 \sum_{\substack{1\leq j\neq i\leq n \\ c_{i,j}=0}} \left| \bigsqcup_{\overline{g}\in G/N(H_j)} \overline{g}H_j\overline{g}^{-1} \setminus \{1\} \right| \\ &= \frac{1}{|G|} m_i^2 \sum_{\substack{1\leq j\neq i\leq n \\ c_{i,j}=0}} \frac{|G|}{|N(H_j)|}(|H_j|-1) = m_i^2 \sum_{\substack{1\leq j\neq i\leq n \\ c_{i,j}=0}} \left(\frac{1}{|W_j|} - \frac{1}{|W_j||H_j|} \right) \end{aligned}$$

Ce qui donne l'inégalité voulue. □

4.3.3 Des inégalités sur les coefficients de Fourier au théorème de Suzuki.

Nous allons maintenant conclure à partir des inégalités du lemme 4.3.8 appliquées à $i = 1$. Quitte à réordonner les groupes H_i (dont l'ordre à été choisi arbitrairement), on peut supposer que :

$$|W_1| \leq |W_2| \leq \cdots \leq |W_n|$$

Alors la proposition 4.2.2 donne que :

$$\begin{aligned} 1 &= \frac{1}{|G|} + \frac{1}{|W_1|} - \frac{1}{|H_1||W_1|} + \sum_{\substack{2\leq j\leq n \\ c_{i,j}\neq 0}} \left(\frac{1}{|W_i|} - \frac{1}{|H_i||W_i|} \right) + \sum_{\substack{2\leq j\leq n \\ c_{i,j}=0}} \left(\frac{1}{|W_i|} - \frac{1}{|H_i||W_i|} \right) \\ &\leq \frac{1}{|G|} + \frac{1}{|W_1|} - \frac{1}{|H_1||W_1|} + \sum_{\substack{2\leq j\leq n \\ c_{i,j}\neq 0}} \frac{1}{|W_2|} + \frac{1}{m_1} \\ &\leq \frac{1}{|G|} + \frac{1}{|W_1|} - \frac{1}{|H_1||W_1|} + \frac{|W_1|-1}{2|W_2|} + \frac{1}{m_1} \quad (\star) \end{aligned}$$

Comme $\frac{1}{|G|} \leq \frac{1}{|N(H_1)|} = \frac{1}{|H_1||W_1|}$ et $\frac{1}{|W_2|} \leq \frac{1}{|W_1|}$, il s'ensuit que :

$$1 \leq \frac{1}{|W_1|} + \frac{|W_1|-1}{2|W_1|} + \frac{1}{m_1} \quad \text{donc} \quad m_1 \leq \frac{1}{\frac{1}{2} - \frac{1}{2|W_1|}}$$

Comme $|W_1| \geq 3$ d'après le lemme 4.2.4, on en déduit que $m_1 \leq 3$. Comme $m_1 = \frac{|H_1|-1}{|W_1|} \geq 2$ est pair, nécessairement $m_1 = 2$ i.e. $|H_1| = 2|W_1| + 1$ et donc en réinjectant ceci dans $(\star)$ on obtient :

$$1 \leq \frac{1}{|G|} + \frac{1}{|W_1|} - \frac{1}{|W_1|(2|W_1|+1)} + \frac{|W_1|-1}{2|W_2|} + \frac{1}{2}$$

Et donc :

$$\frac{1}{2} \leq \frac{1}{|G|} + \frac{2}{2|W_1|+1} + \frac{|W_1|-1}{2|W_2|} \quad (\star\star)$$

On distingue alors deux cas :

Premier cas : Supposons que $|W_2| > |W_1|$. Alors $|W_2| \geq |W_1| + 2$ puisque ces deux entiers sont impairs. On en déduit que :

$$\frac{|W_1|-1}{2|W_2|} \leq \frac{|W_1|-1}{2(|W_1|+2)} = \frac{|W_1|+2-3}{2(|W_1|+2)} = \frac{1}{2} - \frac{3}{2(|W_1|+2)}$$

Et donc par $(\star\star)$:

$$\frac{1}{|G|} \geq \frac{3}{2(|W_1|+2)} - \frac{2}{2|W_1|+1} = \frac{2|W_1|-5}{2(|W_1|+2)(2|W_1|+1)}$$

Puis :

$$|G| \leq \frac{2(|W_1|+2)(2|W_1|+1)}{2|W_1|-5}$$

En outre :

$$|G| \geq |N(H_1)| = |W_1||H_1| = |W_1|(2|W_1|+1)$$

Ainsi :

$$\frac{2(|W_1|+2)(2|W_1|+1)}{2|W_1|-5} \geq |W_1|(2|W_1|+1)$$

inégalité qui devient fausse à partir de $|W_1| \geq 5$. Ainsi, $|W_1| = 3$ et donc :

$$|G| \leq \frac{2 \times (3+2)(2 \times 3+1)}{2 \times 3-5} = 70$$

Pour obtenir une contradiction, nous allons étudier comment $|G|$ se factorise. D'une part, la proposition 4.2.2 donne que :

$$1 = \frac{1}{|G|} + \sum_{i=1}^{n} \left(\frac{1}{|W_i|} - \frac{1}{|W_i||H_i|} \right) \leq \sum_{i=1}^{n} \frac{1}{|W_i|} \leq \frac{1}{3} + \frac{n-1}{5}$$

Donc $n \geq \frac{13}{3}$ donc $n \geq 4$.

D'autre part, on a le :

Lemme 4.3.9. *Les $|H_i|$ $(1 \leq i \leq n)$ sont premiers entre eux deux à deux.*

Démonstration. Supposons par l'absurde que pour $i, j \in [\![1 \ ; \ n]\!]$ distincts, $|H_i|$ et $|H_j|$ ne soient pas premiers entre eux. Alors H_i et H_j admettent un diviseur premier commun p. Soit S est un p-Sylow de G (qui existe d'après le théorème de Sylow prouvé en annexe A.3). D'après le lemme A.3.2 prouvé en annexe A.3, il existe $g_i, g_j \in G$ tels que $K_i := g_i S g_i^{-1} \cap H_i$ et $K_j := g_j S g_j^{-1} \cap H_j$ sont des p-Sylow respectifs de H_i et H_j.

En outre, $Z(S)$ est non trivial. En effet, faisons agir S sur lui-même par conjugaison et posons $|S| := p^\alpha$ avec $\alpha \in \mathbb{N}^*$. Soit $s_1, \cdots, s_k$ un système de représentants des orbites de S. Alors l'équation aux classes donne :

$$p^\alpha = |S| = \sum_{i=1}^{k} |S \cdot s_i|$$

avec pour tout $i \in [\![1 \ ; \ k]\!]$, $S \cdot s_i$ l'orbite de s_i, qui est triviale si et seulement si $s_i \in Z(S)$. Dans le cas contraire, $|S \cdot s_i| = \frac{|S|}{|S_{s_i}|}$ où S_{s_i} est le stabilisateur de s_i qui est un sous-groupe $\subsetneq S$ donc $|S \cdot s_i|$ est une puissance non triviale de p. On en déduit que :

$$|Z(S)| = p^\alpha - \sum_{\substack{1 \leq i \leq k \\ s_i \notin Z(S)}} |S \cdot s_i| \equiv 0 \, [p]$$

Donc $|Z(S)|$ est une puissance non triviale de p et nécessairement non-trivial.

Soit donc $s_0 \in Z(S) \setminus \{1\}$, alors pour tous $s, s' \in S$, s et s' commutent avec s_0 donc entre eux puisque G (donc S) est CA et donc S est abélien.

Mais alors $K_i = g_i S g_i^{-1}$ car sinon, on dispose de $g \in g_i S g_i^{-1} \setminus H_i$ et alors g commute avec tous les éléments de $g_i S g_i^{-1}$ (qui est abélien) donc de K_i donc de H_i qui est abélien et qui contient K_i (par propriété CA de G). Donc le sous-groupe de G engendré par H_i et G est abélien et contient strictement H_i, ce qui contredit la maximalité de H_i. De même $K_j = g_j S g_j^{-1}$. Ainsi, H_i contient un conjugué d'un élément non-trivial de H_j, ce qui contredit le lemme 4.2.1. D'où le résultat. □

Exemple 4.3.10. Ce lemmme se vérifie bien dans le cas de $SL_2(\mathbb{F}_q)$ lorsque q est une puissance de 2 puisque le tore T_2, le groupe unipotent T_2 et le tore non-scindé T_3 ont respectivement pour cardinal $q-1$, q et $q+1$. On a en outre :

$$|T_1||T_2||T_3| = (q-1)q(q+1) = |SL_2(\mathbb{F}_q)|$$

ce qui est en fait un fait général (on a toujours $|G| = \prod_{i=1}^{n} |H_i|$).

L'inégalité $n \geq 4$ et le lemme précédent prouvent que $|G|$ admet 4 facteurs premiers distincts. Ainsi, $|G| \geq 2 \times 3 \times 5 \times 7 = 210$. Ceci contredit le fait que $|G| \leq 70$.

Deuxième cas : $|W_1| = |W_2|$. Alors quitte à interchanger les indices 1 et 2 et appliquer le raisonnement vu au début de ce paragraphe, on obtient que $m_2 = 2 = m_1$. On a alors $|W_1| = |W_2|$ et $\frac{|H_1|-1}{|W_1|} = \frac{|H_2|-1}{|W_2|}$ donc $|H_1| = |H_2|$ ce qui contredit le lemme 4.3.9.

Conclusion : Les deux cas traités conduisent à une contradiction. Ainsi, il n'existe pas de groupe d'ordre impair non-abélien, CA et simple. Ceci prouve le théorème de Suzuki d'après la proposition 4.1.5.

Références

[Cours] Gaëtan Chenevier. *Théorie Algébrique des Nombres*. Palaiseau, École Polytechnique, 2018, 149 p.

[Galois] David Hernandez et Yves Laszlo. *Introduction à la théorie de Galois*. Paris, École Polytechnique, le 12 février 2012, 167 p.

[BlogTao] Terence Tao. The theorems of Frobenius and Suzuki on finite groups. In terrytao.wordpress.com [En ligne]. <https ://terrytao.wordpress.com/2013/04/12/the-theorems-of-frobenius-and-suzuki-on-finite-groups/>, consulté le 25 septembre 2018.

A Prérequis d'algèbre générale.

A.1 Produit tensoriel d'espaces vectoriels.

Soient V et W deux espaces vectoriels sur un même corps K. Le produit tensoriel est l'unique K-espace vectoriel (à isomorphisme près) qui fasse correspondre une forme bilinéaire sur $V \times W$ à une forme linéaire sur cet espace. Il est défini par la propriété universelle qui suit :

Théorème A.1.1. *Il existe un unique K-espace vectoriel E muni d'une application bilinéaire :*

$$\beta : V \times W \longrightarrow E$$

tel que pour tout K-espace vectoriel F et toute application bilinéaire $b : V \times W \longrightarrow F$, il existe une unique application linéaire $f : E \longrightarrow F$ telle que :

$$b = f \circ \beta$$

Comme c'est souvent le cas lorsque l'on énonce une propriété universelle, E est unique à isomorphisme près et on le note donc $E := V \otimes W$ sans ambiguïté. On peut en outre noter $v \otimes w := \beta(v, w)$ pour tout $(v, w) \in V \times W$.

Démonstration. Commençons par montrer qu'une solution (E, β) de la propriété universelle est unique. En effet, soit (E', β') est une (autre) solution. Commençons déjà par remarquer que l'unicité de l'application linéaire f assure que $E = \mathrm{Vect}_K \beta(V \times W)$, la propriété $b = f \circ \beta$ restant vraie si f est modifiée sur un supplémentaire de $\mathrm{Vect}_K \beta(V \times W)$. De même, $E' = \mathrm{Vect}_K \beta'(V \times W)$. En appliquant la propriété universelle à E et E' dans chaque sens, on obtient l'existence de $f : E \longrightarrow E'$ et de $g : E' \longrightarrow E$ linéaires telles que :

$$\beta' = f \circ \beta \quad \text{et} \quad \beta = g \circ \beta'$$

Ainsi, $\beta = g \circ f \circ \beta$ et donc par linéarité et vu que $E = \mathrm{Vect}_K \beta(V \times W)$, on a $g \circ f = \mathrm{id}_E$. De même, $f \circ g = \mathrm{id}_{E'}$ et donc E et E' sont isomorphes.

On donne maintenant une preuve de l'existence. Considérons l'espace $K^{(V \times W)}$ formé des fonctions de $V \times W$ presque nulles i.e. non nulles sur un nombre fini d'éléments de $V \times W$. Alors la famille $(\delta_{(v,w)})_{(v,w) \in V \times W}$ des diracs en $(v, w) \in V \times W$ est une base de cet espace. Cet espace ne convient pas tout à fait car on aimerait pouvoir poser "$v \otimes w := \delta_{(v,w)}$" et obtenir la bilinéarité de cette expression. Nous allons donc quotienter $K^{(V \times W)}$ pour obtenir la bilinéarité voulue. Soit $\mathcal{F}$ le sous-espace vectoriel de $K^{(V \times W)}$ engendré par les $\delta_{(v+v',w)} - \delta_{(v,w)} - \delta_{(v',w)}$, $\delta_{(v,w+w')} - \delta_{(v,w)} - \delta_{(v,w')}$, $\delta_{(\lambda v,w')} - \lambda \delta_{(v,w)}$, $\delta_{(v,\lambda w)} - \lambda \delta_{(v,w)}$ pour $v, v' \in V$, $w, w' \in W$ et $\lambda \in K$. On considère alors :

$$E := K^{(V \times W)} / \mathcal{F}$$

et pour tout $(v, w) \in V \times W$, on prend pour $\beta(v, w)$ la classe de $\delta_{(v,w)}$ modulo $\mathcal{F}$. Alors β est clairement bilinéaire de $V \times W$ dans E par construction. En outre $\beta(V \times W)$ engendre E.

Il s'agit maintenant de vérifier que l'espace E construit vérifie la propriété universelle. Soient F un K-espace vectoriel quelconque et $b : V \times W \longrightarrow F$ bilinéaire. On considère $g : K^{(V \times W)} \longrightarrow F$ l'unique application K-linéaire telle que $g(\delta_{(v,w)}) := b(v, w)$ pour tout $(v, w) \in V \times W$. Par bilinéarité de b, g s'annulle sur $\mathcal{F}$ donc par passage au quotient, g se factorise de manière unique en :

$$g = f \circ \Pi$$

où $\Pi : K^{(V \times W)} \longrightarrow E$ est la réduction canonique et $f : E \longrightarrow F$ est une application K-linéaire. On a alors clairement $f \circ \beta = b$ par construction. L'unicité de f est une conséquence immédiate du fait que $\beta(V \times W)$ engendre E. D'où le résultat. □

Proposition A.1.2. *Si V et W sont des espaces vectoriels de dimension finie n et m respecivement et que $\mathcal{B} := (e_1, \cdots, e_n)$ et $\mathcal{C} := (f_1, \cdots, f_m)$ sont des bases respectives de V et W alors $\mathcal{D} := (e_i \otimes f_j)_{\substack{1\leq i\leq n\\1\leq j\leq m}}$ est une base de $V \otimes W$. Ainsi :*

$$dim(V \otimes W) = dim(V)dim(W)$$

Démonstration. Par construction, $V \otimes W$ est engendré par les produits $v \otimes w$ pour $(v, w) \in V \times W$ et tout élément de V pouvant s'écrire dans la base $\mathcal{B}$ et tout élément de W pouvant s'écrire dans la base $\mathcal{C}$, il s'ensuit que tout élément de $V \otimes W$ peut s'écrire comme combinaison linéaire d'éléments de $\mathcal{D}$ par bilinéarité de l'opérateur produit tensoriel. Donc $\mathcal{D}$ est génératrice et $\dim(V \otimes W) \leq nm$.

Considérons maintenant l'espace $F := M_{n,m}(K)$ et l'unique application bilinéaire $b : V \times W \longrightarrow F$ donnée par $b(e_i, f_j) := E_{i,j}$ pour tous $1 \leq i \leq n$ et $1 \leq j \leq m$ avec :

$$E_{i,j} = (\delta_{i,k}\delta_{j,l})_{\substack{1\leq k\leq n\\1\leq l\leq m}}$$

Alors d'après le théorème précédent, il existe une unique application linéaire $f : V \otimes W \longrightarrow F$ telle que $b = f \circ \beta$. β étant l'application bilinéaire :

$$\beta : (v, w) \in V \times W \longmapsto v \otimes w \in V \otimes W$$

Comme $(E_{i,j})_{\substack{1\leq k\leq n\\1\leq l\leq m}}$ est une base de $F = M_{n,m}(K)$, f est nécessairement surjective. Il s'ensuit que $\dim(V \otimes W) \geq \dim(F) = nm$. Donc :

$$\dim(V \otimes W) = nm = \dim(V)\dim(W)$$

et $\mathcal{D}$ est une base de $V \otimes W$. □

Proposition A.1.3 (produit tensoriel d'applications linéaires)**.** *Soient $f \in L(V_1, V_2)$ et $g \in L(W_1, W_2)$ deux applications linéaires. Alors il existe une unique application linéaire $h \in L(V_1 \otimes W_1, V_2 \otimes W_2)$ telle que :*

$$\forall (v, w) \in V_1 \times W_1, \quad h(v \otimes w) = f(v) \otimes f(w)$$

On note $f \otimes g$ cette application linéaire.

Démonstration. L'application $b : (v, w) \in V_1 \times W_1 \longmapsto f(v) \otimes f(w) \in V_2 \otimes W_2$ est bilinéaire donc si l'on désigne par β l'opérateur bilinéaire produit tensoriel sur $V_1 \times W_1$, on obtient par le théorème A.1.1 l'existence et l'unicité de $h \in L(V_1 \otimes W_1, V_2 \otimes W_2)$ telle que $b = h \circ \beta$. On a donc bien :

$$\forall (v, w) \in V_1 \times W_1, \quad h(v \otimes w) = f(v) \otimes f(w)$$

□

Remarque A.1.4. Il peut y avoir confusion sur la notation car $f \otimes g$ désigne aussi un élément de $L(V_1, V_2) \otimes L(W_1, W_2)$. Pour que ceci ait un sens, il faudrait donc vérifier que l'on puisse identifier chaque application linéaire $h =$"$f \otimes g$" de $L(V_1 \otimes W_1, V_2 \otimes W_2)$ à son homologue $f \otimes g$ de $L(V_1, V_2) \otimes L(W_1, W_2)$. Or, on associe au couple (f, g) un unique objet $f \otimes g$ de $L(V_1, V_2) \otimes L(W_1, W_2)$ par construction et l'application $(f, g) \in L(V_1, V_2) \times L(W_1, W_2) \longmapsto h \in L(V_1 \otimes W_1, V_2 \otimes W_2)$ est injective donc l'identification ne pose aucun problème.

Proposition A.1.5. *Soient V, W des espaces vectoriels de dimension finie dont $\mathcal{B} := (e_i)_{1\leq i\leq n}$ et $\mathcal{C} := (f_j)_{1\leq j\leq m}$ sont des bases respectives. Si $f \in L(V)$ et $g \in L(W)$ ont pour matrices respectives $A \in M_n(K)$ et $B \in M_m(K)$ dans les bases $\mathcal{B}$ et $\mathcal{C}$ respectivement alors $f \otimes g$ a pour matrice dans la base*

$\mathcal{D} := (e_i \otimes f_j)_{\substack{1\leq i\leq n \\ 1\leq j\leq m}}$ *de* $V \otimes W$*, le produit de Kronecker :*

$$A \otimes B := (A_{i,j}B)_{1\leq i,j\leq n}$$

Démonstration. On a pour $1 \leq i \leq n$ et $1 \leq j \leq m$ fixés :

$$(f \otimes g)(e_i \otimes f_j) = f(e_i) \otimes g(f_j) = \left(\sum_{k=1}^{n} A_{k,i}e_k\right) \otimes \left(\sum_{l=1}^{m} B_{l,j}f_l\right) = \sum_{\substack{1\leq k\leq n \\ 1\leq l\leq m}} A_{k,i}B_{l,j}e_k \otimes f_l$$

L'écriture de la matrice de $f \otimes g$ dans $\mathcal{D}$ s'en déduit immédiatement. □

A.2 Produit semi-direct de groupes.

A.2.1 produit interne

On commence par rappeler ici quelques propriétés des sous-groupes engendrés par des parties au sein d'un groupe

Notamment, on considère pour H et K deux sous groupes d'un groupe noté multiplicativement, alors $< H \cup K >$ correspond à l'ensemble des produits finis d'éléments de H et de K

On a alors naturellement $HK \subset < H \cup K >$. Cela dit HF n'est à priori pas un sous-groupe.

Lemme A.2.1. *Si un des deux sous groupes est distingué, l'inclusion précédente est une égalité.*

Il suffit d'expliciter le cas où on considère un élément $h_1f_1h_2f_2$ puis on procède par récurrence sur le nombre de facteurs mis en jeu

Le caractère distingué donne $h_1f_1h_2f_1^{-1} \in H$ ce qui permet de conclure

Si on a de plus $H \cup K = e$ on a unicité de l'écriture $g \in G = hk$ et on dit que G est le produit semi-direct de K et H

La loi de groupe vue comme produit s'explicite de la même façon que dans la preuve du lemme précédent

On reprendra ce genre de construction pour la définition des produits semi-directs externes

A.2.2 Produit semi-direct externe

On prend de manière plus générale F et H comme deux groupes, ainsi que ϕ un morphisme de F dans $Aut(F, H)$

Forts de ceci on va construire un groupe G qui contiendra F et H comme sous-groupes et qui vérifiera les conditions du produit semi-direct interne

Remarque : G ne contient pas à proprement parler les deux groupes. Mais on les plonge dedans via des morphismes injectifs.

Plus précisément : ϕ est un morphisme de K dans $Aut(H)$ On munit $H \times K$ d'un produit interne comme suit $(h_1, f_1)(h_2, f_2) = (h_1\phi(f_1)(h_2), f_1f_2)$ où $\phi(f)$ agit comme l'automorphisme intérieur de conjuguaison par h

On plonge H et K dans ce produit via les morphismes i et j définis comme envoyant respectivement h sur (h, e) et g sur (e, g)

Une différence fondamentale entre le produit externe et le produit interne concerne ϕ Dans le cas interne, ϕ est imposé par la situation comme étant le morphisme associant l'automorphisme de conjuguaison. Dans le cas externe, on le choisit a priori et on construit le groupe produit de sorte qu'il soit la restriction de ce morphisme

A.3 Théorèmes de Sylow

Voici un prérequis de théorie des groupes important, dont l'usage est courant dans les preuves de théorie de groupes finis.

A.3.1 Enoncé des théorèmes

On les donne souvent au nombre de 3. On se donne pour cela un groupe G de cardinal fini n, et p un diviseur premier de n de sorte que $n = p^r s$ où $s \neq 0[p]$

Ainsi on appelle p-Sylow de G un sous-groupe de cardinal p^r Et on note $S_p(G)$ l'ensemble des p-Sylow de G

Théorème A.3.1. *premier théorème G admet des p-Sylow.*

Pour les énoncés suivants on utilisera le lemme

Lemme A.3.2. *Si S est un p-Sylow et H un sous groupe d'ordre divisible par p, alors on peut trouver $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H*

Théorème A.3.3. *Théorèmes 2 et 3 Tous les p-Sylow sont conjugués et sous p-groupe de G est contenu dans un p-sylow.*

$|S_p(G)| \equiv 1[p]$ *et* $|S_p(G)| \nmid s$

Ces théorèmes structurent largement $S_p(G)$

A.3.2 Preuves

Avec les notations de son énonce, On note X un ensemble de représentants de sorte qu'on ait

$$G = \bigsqcup_{x \in X} HxS = \bigsqcup_{x \in X} \bigsqcup_{h \in H/xSx^{-1} \cap H} hxS$$

Puis

$$|G| = \sum_{x \in X} |S|[H : xSx^{-1} \cap H]$$

Donc

$$[G : S] = \sum_{x \in X} [H : xSx^{-1} \cap H]$$

Or par hypothèse p ne divise pas $[G : S]$ donc un des termes de la somme, ce qui signifie que pour un $x_0 \in X$, on a, puisque p divise $|H|$, $x_0 S x_0^{-1} \cap H$ est un p-Sylow de H

On procède par récurrence sur le cardinal du groupe en considérant l'action de G sur lui même par automorphismes intérieurs, l'équation aux classes fournit.

$$|G| = |Z(G)| + \sum_i [G : H_i]$$

En ayant considéré les H_i comme les centralisateurs des représentants choisis.

Ainsi, supposons qu'on ait un des indices tel que $p \nmid [G : H_i]$, alors $|H_i|$ est de la forme $p^r s'$ où $s' < s$, on conclut donc par récurrence, un p-Sylow de H_i étant un p-Sylow de G

Sinon, on a $p||Z(G)|$ de sorte que $G/Z(G)$ est un groupe de cardinal strictement inférieur auquel on applique l'hypothèse de récurrence, il suffit alors de relever le p-Sylow obtenu dans G

On prouve maintenant les théorèmes 2 et 3

On applique le lemme à S et S' deux p-Sylow de G, un p-Sylow d'un p-groupe étant naturellement tout le groupe.

L'action de conjugaison sur $S_p(G)$ étant transitive, on peut écrire pour S un p-Sylow une surjection naturelle de G/S sur $G/Nor_G(S)$ qui est isomorphe à $S_p(G)$ Il vient que $|S_p(G)|$ divise $|G/S| = s$

On peut également faire agir S par conjugaison sur $S_p(G)$, $S \cdot S'$ est d'ordre une puissance de p pour tout p-Sylow S' or :

$$|S_p(G)| = \sum_{S' \in S_p(G)} |S \cdot S'|$$

Montrons que seule la classe de S est d'ordre 1

Autrement on aurait $sS's^{-1} = S'$ pour un $s \in S$, et alors SS' serait un p-groupe contenant strictement S

B Etude du groupe $SL_2(\mathbb{F}_q)$ lorsque q est une puissance de 2.

Faisons une remarque préliminaire concernant $\mathbb{F}_q$ lorsque q est une puissance de 2. Nous serons amenés à diagonaliser et à trigonaliser les matrices de $SL_2(\mathbb{F}_q)$ ce qui rendra nécessaire l'étude de leur polynôme caractéristique. Nous sommes en caractéristique 2 donc on ne peut plus trouver les racines des polynômes de degré 2 dans une extension quadratique de type $\mathbb{F}_q[\sqrt{d}]$ (où la racine carré du discriminant existe) et utiliser des expressions de la forme $\frac{-b\pm\sqrt{\Delta}}{2a}$. Nous allons travailler dans d'autres types d'extensions quadratiques.

On considère la fonction $f : x \in \mathbb{F}_q \longmapsto x^2 + x \in \mathbb{F}_q$. Pour tout $y \in \mathrm{im}(f)$, y a deux antécédants $x_0, x_1 \in \mathbb{F}_q$ qui sont les racines du polynôme $X^2 + X + y$. Ces deux racines sont distinctes car sinon, on aurait :

$$X^2 + X + y = (X - x_0)^2 = X^2 - 2x_0X + x_0^2 = X^2 + x_0^2$$

Ainsi, le lemme des bergers assure que $|\mathrm{im}(f)| = \frac{q}{2}$. On dispose donc de $y \in \mathbb{F}_q \setminus \mathrm{im}(f)$, qui est non nul car $0 = f(0)$. Le polynôme $X^2 + X + y$ est alors irréductible, et on peut donc prendre comme extension quadratique, $\mathbb{F}_{q^2} := \mathbb{F}_q[X]/(X^2 + X + y) = \mathbb{F}_q[\xi]$ où ξ est la classe de X modulo $X^2 + X + y$. Tous les polynômes de degré 2 de $\mathbb{F}_q[X]$ étant scindés dans une certaine extension quadratique de degré 2 et toutes ces extensions étant isomorphes, il s'ensuit que tous les polynômes de degré 2 de $\mathbb{F}_q[X]$ sont scindés dans $\mathbb{F}_q[\xi]$.

Proposition B.0.1. **(i)** *Les matrices de $SL_2(\mathbb{F}_q)$ sont toutes conjuguées (dans $SL_2(\mathbb{F}_q)$) à une matrice de l'un des types suivants :*

type 1 : $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ *pour* $\lambda \in \mathbb{F}_q^*$.

type 2 : $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ *pour* $x \in \mathbb{F}_q$.

type 3 : $\begin{pmatrix} \alpha & \beta \\ \beta y & \alpha + \beta \end{pmatrix}$ *avec* $\alpha, \beta \in \mathbb{F}_q$ *tels que* $\alpha^2 + \alpha\beta + \beta^2 y = 1$.

seule l'identité I_2 étant dans plusieurs types. On notera T_i l'ensemble des matrices de type i pour $i \in \{1, 2, 3\}$.

(ii) *Si $M = PTP^{-1}$ avec $P \in SL_2(\mathbb{F}_q)$ et $T \in T_i \setminus \{I_2\}$ pour $i \in \{1, 2, 3\}$ alors le commutant de M dans $SL_2(\mathbb{F}_q)$ est $Z(M) = PT_iP^{-1}$.*

(iii) *T_1, T_2 et T_3 sont des sous-groupes abéliens maximaux de $SL_2(\mathbb{F}_q)$ de cardinaux respectifs $q - 1$, q et $q + 1$ appelés respectivement* tore, groupe unipotent *et* tore non-scindé.

Remarque B.0.2. Cette proposition prouve en particulier que $SL_2(\mathbb{F}_q)$ est commutant abélien.

Démonstration. **(i)** Soit $M \in SL_2(\mathbb{F}_q)$. Alors on distingue 3 cas :

Premier cas : Si M est diagonalisable sur $\mathbb{F}_q$ alors elle est clairement conjuguée dans $GL_2(\mathbb{F}_q)$ à une matrice de type 1. Si l'on note P la matrice de similitude alors quitte à diviser la première colonne de P par $\det(P)$, on peut supposer que $P \in SL_2(\mathbb{F}_q)$ donc M est en fait conjugué à une matrice de type 1 dans $SL_2(\mathbb{F}_q)$.

Deuxième cas : Si M est trigonalisable sur $\mathbb{F}_q$ alors ses deux valeurs propres sont identiques et vérifient $\lambda^2 = \det(M) = 1$ de sorte que $\lambda = \pm 1 = 1$ donc M est conjuguée dans $GL_2(\mathbb{F}_q)$ (donc dans $SL_2(\mathbb{F}_q)$) à une matrice de type 2.

Troisième cas : Supposons que M ne soit ni diagonalisable ni trigonalisable sur $\mathbb{F}_q$. On sait qu'alors $\chi_M = X^2 - \mathrm{Tr}(M)X + 1$ est scindé sur $\mathbb{F}_q[\xi]$ par deux valeurs propres $\lambda = \alpha + \beta\xi$ et $\mu = \gamma + \delta\xi$ avec $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ et $\beta\delta \neq 0$ car $\lambda, \mu \notin \mathbb{F}_q$ (sinon χ_M serait scindé sur $\mathbb{F}_q$ et M serait diagonalisable

ou trigonalisable sur $\mathbb{F}_q$). On a alors $\lambda\mu = 1$ donc :

$$(\alpha+\beta\xi)(\gamma+\delta\xi) = 1 \iff \alpha\gamma + \beta\delta \underbrace{\xi^2}_{\xi+y} + (\alpha\delta+\beta\gamma)\xi = 1 \iff \left\{ \begin{array}{c} \alpha\delta+\beta\gamma+\beta\delta = 0 \\ \alpha\gamma+\beta\delta y = 1 \end{array} \right.$$

$$\iff \left\{ \begin{array}{c} \gamma = \frac{\delta}{\beta}(\alpha+\beta) \\ \alpha\frac{\delta}{\beta}(\alpha+\beta)+\beta\delta y = 1 \end{array} \right. \iff \left\{ \begin{array}{c} \gamma = \frac{\delta}{\beta}(\alpha+\beta) \\ \delta(\alpha^2+\alpha\beta+\beta^2 y) = \beta \end{array} \right.$$

$$\iff \alpha^2+\alpha\beta+\beta^2 y \neq 0 \text{ et } \left\{ \begin{array}{l} \gamma = \frac{\alpha+\beta}{\alpha^2+\alpha\beta+\beta^2 y} \\ \delta = \frac{\beta}{\alpha^2+\alpha\beta+\beta^2 y} \end{array} \right.$$

où l'on a utilisé le fait que $(1, \xi)$ est une $\mathbb{F}_q$-base de $\mathbb{F}_q[\xi]$. Comme $\lambda + \mu = \mathrm{Tr}(M)$, on a nécessairement :

$$\beta+\delta = \beta+\frac{\beta}{\alpha^2+\alpha\beta+\beta^2 y} = 0 \iff \beta(\alpha^2+\alpha\beta+\beta^2 y+1) = 0 \iff \alpha^2+\alpha\beta+\beta^2 y = -1 = 1 \text{ car } \beta \neq 0$$

Ainsi, $\lambda = \alpha+\beta\xi$ et $\mu = \alpha+\beta+\beta\xi$. Ces deux valeurs propres sont donc distinctes (car sinon $\beta = 0$) et donc M est en fait diagonalisable sur $\mathbb{F}_q[\xi]$. Donc :

$$M = P\mathrm{Diag}(\alpha+\beta\xi, \alpha+\beta+\beta\xi)P^{-1}$$

avec $P \in GL_2(\mathbb{F}_q[\xi])$. Quitte à diviser la première colonne de P par $\det(P)$, on peut supposer $P \in SL_2(\mathbb{F}_q[\xi])$. On peut alors écrire $P := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a, b, c, d \in \mathbb{F}_q[\xi]$ tels que $\det(P) = ad - bc = 1$ et $P^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ de sorte que :

$$M = \begin{pmatrix} ad(\alpha+\beta\xi) - bc(\alpha+\beta+\beta\xi) & -ac(\alpha+\beta\xi) + ac(\alpha+\beta+\beta\xi) \\ bd(\alpha+\beta\xi) - bd(\alpha+\beta+\beta\xi) & -bc(\alpha+\beta\xi) + ad(\alpha+\beta+\beta\xi) \end{pmatrix}$$
$$= \begin{pmatrix} \alpha+\beta\xi+\beta bc & \beta ac \\ \beta bd & \alpha+\beta+\beta bc+\beta\xi \end{pmatrix}$$

Comme M est à coefficients dans $\mathbb{F}_q$, il s'ensuit que $bc = \xi$, $ac \in \mathbb{F}_q$ et $bd \in \mathbb{F}_q$, puis que $ad = 1+\xi$, de sorte que $abcd = \xi^2+\xi = y$, puis que $bd = \frac{y}{ac}$. Donc :

$$M = \begin{pmatrix} \alpha & \beta ac \\ \beta\frac{y}{ac} & \alpha+\beta \end{pmatrix} = \mathrm{Diag}\left(\sqrt{ac}, \frac{1}{\sqrt{ac}}\right) \begin{pmatrix} \alpha & \beta \\ \beta y & \alpha+\beta \end{pmatrix} \mathrm{Diag}\left(\frac{1}{\sqrt{ac}}, \sqrt{ac}\right)$$

Si $q = 2$ alors $ac = 1$ donc M est de type 3. Sinon, M est semblable à une matrice de type 3 dans $GL_2(\mathbb{F}_q[\xi])$, donc dans $GL_2(\mathbb{F}_q)$ d'après le lemme qui suit, donc dans $SL_2(\mathbb{F}_q)$ (d'après la remarque du premier cas).

Lemme B.0.3. *Si $q \geq 4$ et si $M, N \in M_2(\mathbb{F}_q)$ sont semblables dans $GL_2(\mathbb{F}_q[\xi])$ alors elles sont semblables dans $GL_2(\mathbb{F}_q)$.*

Démonstration. Il s'agit d'étudier le système $(S) : PM - NP = 0$ d'inconnue $P \in M_2(\mathbb{F}_q)$ pour montrer qu'il admet une solution dans $GL_2(\mathbb{F}_q)$. Ce système à 4 inconnues admet une solution non nulle dans $M_2(\mathbb{F}_q[\xi])$ donc son rang r dans $\mathbb{F}_q[\xi]$ (qui est le rang de sa matrice dans la base canonique) est ≤ 3. Or, par invariance du rang par extension de corps [5], le rang de (S) dans $\mathbb{F}_q$ est aussi $r \leq 3$. Posons $m := 4-r > 0$. Alors on dispose de $(P_1, \cdots, P_m)$ une $\mathbb{F}_q$-base de l'espace des solutions de (S) dans $M_2(\mathbb{F}_q)$, qui est aussi

5. On rappelle ici l'argument : le rang d'une matrice est la taille maximale de ses sous-matrices inversibles. Or, l'inversibilité d'une matrice de $M_2(\mathbb{F}_q)$ dans $\mathbb{F}_q[\xi]$ est équivalente à l'inversibilité dans $\mathbb{F}_q$ puisqu'elle équivaut à la non-nullité du déterminant.

une $\mathbb{F}_q[\xi]$-base de l'espace des solutions de (S) dans $M_2(\mathbb{F}_q[\xi])$, toujours par invariance du rang par extension de corps.

Considérons le polynôme $R := \det(X_1P_1 + \cdots + X_mP_m) \in \mathbb{F}_q[X_1, \cdots, X_m]$. (S) admet une solution $Q \in GL_2(\mathbb{F}_q[\xi])$ qui s'écrit $Q = \sum_{i=1}^m \mu_i P_i$ avec $\mu_1, \cdots, \mu_m \in \mathbb{F}_q[\xi]$, donc $R(\mu_1, \cdots, \mu_m) = \det(Q) \neq 0$. Ainsi, R est non-nul.

Il s'agit maintenant de montrer que R est non nul sur $\mathbb{F}_q^m$. Car alors on pourra prendre $P := \sum_{i=1}^m \lambda_i P_i$ comme solution de (S) convenable pour $(\lambda_1, \cdots, \lambda_m) \in \mathbb{F}_q^m$ non-annulateur de R. On aura alors $\det(P) = R(\lambda_1, \cdots, \lambda_m) \neq 0$ donc $P \in GL_2(\mathbb{F}_q)$.

Supposons par l'absurde que R soit nul sur $\mathbb{F}_q^m$ tout entier. Remarquons que R est de degré au plus 2 en chacune de ses variables. Ainsi, on peut écrire :

$$R(X_1, \cdots, X_m) = X_1^2 R_2(X_2, \cdots, X_m) + X_1 R_1(X_2, \cdots, X_m) + R_0(X_2, \cdots, X_m)$$

avec $R_0, R_1, R_2 \in \mathbb{F}_q[X_2, \cdots, X_m]$. Pour $(x_2, \cdots, x_m) \in \mathbb{F}_q^{m-1}$ fixé, le polynôme $R(X_1, x_2, \cdots, x_m)$ est identiquement nul sur F_q donc admet $q \geq 4$ racines. Comme il est de degré au plus 2, il est donc nul et il s'ensuit que R_0, R_1, R_2 s'annulent en $(x_2, \cdots, x_m)$ et ce quel que soit $(x_2, \cdots, x_m) \in \mathbb{F}_q^{m-1}$. On conclut par récurrence, qu'en fait, R est nul, ce qui est absurde. D'où le résultat. □

(ii) Il suffit de prouver le résultat pour des matrices de type $1, 2, 3$. Le résultat pour les conjugués s'en déduit immédiatement.

Soit $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$. Alors si $N := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in SL_2(\mathbb{F}_q)$ commute avec $M := \mathrm{Diag}(\lambda, \lambda^{-1})$, on a :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \mathrm{Diag}(\lambda, \lambda^{-1}) = \begin{pmatrix} \lambda a & \lambda c \\ \lambda^{-1} b & \lambda^{-1} d \end{pmatrix} = \mathrm{Diag}(\lambda, \lambda^{-1}) \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda^{-1} c \\ \lambda b & \lambda^{-1} d \end{pmatrix}$$

donc $b = c = 0$ puisque $\lambda \neq 1$. Puis, $ad = \det(N) = 1$ donc $a \neq 0$ et $d = a^{-1}$. Ainsi, N est de type 1. Réciproquement, une matrice de type 1 commute avec M. D'où $Z(M) = T_1$.

Soit $x \in \mathbb{F}_q^*$. Alors si $N := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in SL_2(\mathbb{F}_q)$ commute avec $M := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, on a :

$$MN = \begin{pmatrix} a + bx & c + dx \\ b & d \end{pmatrix} = NM = \begin{pmatrix} a & ax + c \\ b & bx + d \end{pmatrix}$$

Donc $b = 0$ et $d = a$. Mais alors $a^2 = \det(N) = 1$ donc $a = \pm 1 = 1$ et N est de type 2. Réciproquement, toute matrice de type 2 commute avec M. D'où $Z(M) = T_2$.

Soient $M := \begin{pmatrix} \alpha & \beta \\ \beta y & \alpha + \beta \end{pmatrix}$ avec $\alpha, \beta \in \mathbb{F}_q$ tels que $\alpha^2 + \alpha\beta + \beta^2 y = 1$ une matrice de type 3, distincte de I_2, et $N := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in SL_2(\mathbb{F}_q)$. Alors N commute avec M si et seulement si :

$$MN = \begin{pmatrix} a\alpha + \beta b & \alpha c + \beta d \\ \beta a y + (\alpha + \beta) b & \beta c y + (\alpha + \beta) d \end{pmatrix} = NM = \begin{pmatrix} a\alpha + \beta c y & a\beta + c(\alpha + \beta) \\ \alpha b + \beta d y & \beta b + (\alpha + \beta) d \end{pmatrix}$$

ce qui équivaut à $b = cy$ et $d = a + c$, i.e. N est de type 3. Ainsi, $Z(M) = T_3$.

(iii) Le commutant de tout élément étant toujours un sous-groupe, nous venons de montrer que T_1, T_2 et T_3 sont des groupes de $SL_2(\mathbb{F}_q)$ (à condition pour T_3, que T_3 soit non réduit à $\{I_2\}$, ce que le calcul des cardinaux nous assurera). Ils sont en fait abéliens puisque nous venons aussi de montrer que deux éléments de même types commutent. Ainsi, $SL_2(\mathbb{F}_q)$ est CA d'après (ii) (les conjugués de groupes abéliens étant abéliens). Or, nous avons vu que dans un groupe CA, les commutants d'un élément sont toujours des groupes abéliens maximaux.

Calculons maintenant les cardinaux. Bien-sûr, choisir un élément de T_1 équivaut à choisir $\lambda \in \mathbb{F}_q^*$ donc $|T_1| = q - 1$. Puis, choisir un élément de T_2 revient à choisir $x \in \mathbb{F}_q$ donc $|T_2| = q$. Enfin, choisir un élément de T_3 revient à choisir $(\alpha, \beta) \in \mathbb{F}_q^2$ tel que $\alpha^2 + \alpha\beta + \beta^2 y = (\alpha + \beta\xi)(\alpha + \beta + \beta\xi) = 1$. Si $\beta \neq 0$, ceci revient à choisir une racine d'un polynôme de la forme $X^2 - \beta X + 1 \in \mathbb{F}_q[X]$ irréductible sur $\mathbb{F}_q$. Il y a au total q polynômes de la forme $X^2 - bX + 1$ avec $b \in \mathbb{F}_q$ parmi lesquels il faut compter tous les non-irréductibles, qui sont de la forme $(X - \lambda)(X - \lambda^{-1})$ pour $\lambda \in \mathbb{F}_q^*$. Il y a au total $\frac{q-2}{2}$ tels polynômes pour $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ (en comptant les redondances issues de l'échange $\lambda \leftrightarrow \lambda^{-1}$) auquel il faut ajouter le polynôme $(X - 1)^2$, ce qui donne $\frac{q}{2}$ polynômes non-irréductibles et donc $\frac{q}{2}$ polynômes irréductibles. Puisque chaque polynôme irréductible $X^2 - \beta X + 1 \in \mathbb{F}_q[X]$ pour $\beta \neq 0$ admet deux racines distinctes (puisque $\beta \neq 0$), il y a en fait $2\frac{q}{2} = q$ couples $(\alpha, \beta) \neq (1, 0)$ convenables, ce qui donne $q + 1$ éléments de T_3 en comptant I_2. Ainsi, $|T_3| = q + 1$. □