Rapport du stage de fin de licence
effectué du 10 mai au 11 juin 2010
au laboratoire de mathématiques
de Clermont-Ferrand

Théorie des représentations et théorie des caractères appliquées au cas de $\mathrm{GL}_2(\mathbb{F}_q)$

Arthur CHASSANIOL

le 30 juin 2010

Table des matières

1 Introduction et définitions

1.1 Introduction

La théorie des représentations des groupes est un outil pour étudier les groupes et leurs propriétés. Grâce à [SIN] nous verrons différentes propriétés constructives des représentations et caractères des groupes finis puis nous nous intéresserons plus particulièrement au cas de $\mathrm{GL}_2(\mathbb{F}_q)$ grâce à [PRA].

1.2 Quelques définitions et exemples

Dans cette partie on va définir toutes les notions importantes pour l'étude des représentations. On prendra pour tout ce qui suit G un groupe fini.

Définition 1.2.1 (représentation)**.** Une représentation de G sur un corps k est un couple (π, V) où V est un k-espace vectoriel et π un morphisme de groupes de G dans $\mathrm{GL}(V)$. On dit aussi que π est une représentation de G sur V. La dimension de V est appelée le degré de la représentation.

Dans cette exposé on ne parlera que des représentations de degré fini, ce qui, nous le verrons, est suffisant pour décrire les représentations des groupes finis et nous n'étudierons que les représentations sur $\mathbb{C}$.

Définition 1.2.2 (somme directe de représentations)**.** Soient (π, V) et (π', V') deux représentations de G. On définit de façon naturelle $(\pi \oplus \pi', V \oplus V')$ la somme directe de ces représentations par $(\pi \oplus \pi')(g)(v + v') = \pi(g)(v) + \pi'(g)(v')$.

On vérifie rapidement que $(\pi \oplus \pi', V \oplus V')$ est encore une représentation de G de degré $\dim(V) + \dim(V')$.

Définition 1.2.3 (G-morphisme)**.** Si (π, V) et (τ, U) sont deux représentations de G, un G-morphisme de (π, V) dans (τ, U) est une application linéaire $T : V \to U$, telle que :

$$\forall g \in G, \quad \tau(g)T = T\pi(g).$$

Si T est inversible on dit alors que les représentations (π, V) et (τ, U) sont isomorphes. L'ensemble des G-morphismes de U dans V est noté $\mathrm{Hom}_G(\tau, \pi)$ et celui des G-morphismes de V dans V $\mathrm{End}_G(\pi)$.

Définition 1.2.4 (espace G-invariant)**.** Soient (π, V) une représentation de G et $W \subset V$ un sous-espace de V. On dit que W est G-invariant (ou G-stable) si :

$$\forall w \in W,\ \forall g \in G \quad \pi(g)(w) \in W.$$

Notons que lorsque l'on a un tel espace W on peut restreindre la représentation (π, V) en une représentation (π_W, W) de G en posant $\pi_W(g) = \pi(g)_{|W}$.

Définition 1.2.5 (représentation irréductible)**.** Une représentation irréductible est une représentation (π, V) telle que $V \neq \{0\}$ et qui admet comme seuls sous-espaces G-invariants $\{0\}$ et V.

Définition 1.2.6 (représentation totalement réductible)**.** Soit (π, V) une représentation, on dit qu'elle est totalement réductible si elle est somme directe de représentations irréductibles, c'est-à-dire si $V = W_1 \oplus \cdots \oplus W_r$, avec W_i G-invariant et (π_{W_i}, W_i) représentation irréductible de G.

Après ces premières définitions regardons un exemple de représentation non-triviale du groups $\mathfrak{S}_n$:

Exemple 1.2.7. Pour $G = \mathfrak{S}_n$ on a la représentation naturelle $(\pi, \mathbb{C}^n)$ avec $\pi(\sigma)(e_i) = e_{\sigma(i)}$ où $(e_1, ..., e_n)$ est la base canonique de $\mathbb{C}^n$. On remarque alors que $W =< (1, 1, ..., 1) >$ et $Y = \{(x_1, ..., x_n) | \sum x_i = 0\}$ sont deux sous-espaces G-invariants irréductibles (complémentaires dans $\mathbb{C}^n$) . $(\pi, \mathbb{C}^n)$ est donc la somme directe des deux représentations irréductibles induites sur W et Y.

On note $\hat{G}$ l'ensemble des représentations de G de degré 1, c'est-à-dire l'ensemble des morphismes de groupes de G dans $\mathbb{C}^*$. $\hat{G}$ est un groupe muni de la multiplication suivante : $\forall \chi_1, \chi_2 \in \hat{G},\ \forall g \in G$

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g).$$

De plus on note $\mathbb{C}[G]$ l'ensemble des applications de G dans $\mathbb{C}$, un espace vectoriel de dimension $|G|$. Et on note $\mathcal{H}$ le sous-espace vectoriel de $\mathbb{C}[G]$ des applications constantes sur les classes de conjugaison de G. La dimension de $\mathcal{H}$ est le nombre de classes de conjugaison de G. On définit un produit scalaire hermitien $\langle , \rangle : \mathbb{C}[G] \times \mathbb{C}[G] \to \mathbb{C}$ par :

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{t \in G} f_1(t)\overline{f_2(t)}.$$

Exemple 1.2.8. Un exemple important de représentation est la "représentation régulière". Soit G un groupe d'ordre n. On pose $V = \mathbb{C}[G]$, espace vectoriel de dimension n. On définit alors $\pi : G \to \mathrm{GL}(V)$ par $(\pi(g)(f))(h) = f(g^{-1}h)$. (π, V) est une représentation de G de degré n et le morphisme $\pi : G \to \mathrm{GL}(V)$ est injectif ce qui par définition veut dire que la représentation (π, V) est fidèle.

Voici enfin la définition d'un objet très important dans la théorie des représentations.

Définition 1.2.9 (caractère)**.** Soit (π, V) une représentation de G. Le caractère associé à cette représentation est l'élément χ de $\mathbb{C}[G]$ défini par :

$$\chi(g) = \mathrm{tr}(\pi(g)).$$

Remarque 1.2.10. Si (π, V) et (π', V') sont deux représentations de G de caractères respectifs χ et χ', on vérifie aisément que le caractère associé à $(\pi \oplus \pi', V \oplus V')$ est $\chi + \chi'$.

2 Théorie des caractères

Voici quelques théorèmes importants qui vont nous permettre de mieux comprendre comment construire l'ensemble des représentations d'un groupe notamment à l'aide des caractères associés.

2.1 Résultats généraux

Théorème 2.1.1 (Théorème de Maschke)**.** *Soit* (π, V) *une représentation de degré fini de* G *et* W *un sous espace* G*-invariant de* V*. Alors il existe* W' G*-invariant tel que* $V = W \oplus W'$*.*

Remarque 2.1.2. Ce théorème n'est pas valable pour les représentations sur un corps k quelconque, il utilise le fait que $\mathbb{C}$ est un corps de caractéristique nulle.

On a donc par récurrence sur le degré, la proposition fondamentale suivante :

Proposition 2.1.3. *Toute représentation de degré fini d'un groupe fini est complètement réductible.*

On va donc pouvoir se restreindre à la recherche des représentations irréductibles d'un groupe.

Remarque 2.1.4. De plus toute représentation admet une sous-représentation de degré fini ce qui montre que toute représentation irréductible est de degré fini.

Voici maintenant un lemme et une proposition faciles mais très utiles dans de nombreuses démonstrations.

Lemme 2.1.5 (Lemme de Schur)**.** *[SIN, Proposition 4.3] Soient* (π, V) *et* (π', V') *deux représentations irréductibles de* G*. Si* T *est un* G*-morphisme de* (π, V) *vers* (π', V')*, alors* $T = 0$ *ou* T *est un isomorphisme.*

Proposition 2.1.6. *[SIN, Corollaire 4.5] Soient* (π, V) *une représentation irréductible de* G *et* $T : V \to V$ *un* G*-morphisme. Alors* $\exists \lambda \in \mathbb{C}$ *tel que* $T = \lambda \cdot \mathrm{Id}_V$*.*

La démonstration utilise le fait que tout endomorphisme d'un espace vectoriel complexe admet une valeur propre λ (car $\mathbb{C}$ est algébriquement clos) et que $\ker(T-\lambda \cdot \mathrm{Id}_V)$ est un sous-espace G-invariant de V.

De plus on a le résultat suivant :

Proposition 2.1.7. *Soit* (π, V) *une représentation de* G. (π, V) *est irréductible si et seulement si* $\dim \mathrm{End}_G(\pi) = 1$.

Démonstration. La proposition 2.1.6 montre le sens de gauche à droite de l'équivalence. Montrons l'autre sens par contraposée. Soit (π, V) une représentation de G que l'on suppose non-irréductible. Alors il existe W un sous-espace propre de V G-invariant, puis par le théorème de Maschke il existe W' un autre sous-espace de V G-invariant tel que $V = W \oplus W'$. On considère maintenant T l'endomorphisme de V correspondant à la projection sur W. Donc si $x = w + w' \in V$ on a par G-invariance de W et W' :

$\forall g \in G,\ \pi(g)T(x) = \pi(g)(w) = T(\pi(g)(w)) = T(\pi(g)(x - w')) = T(\pi(g)(x) - \pi(g)(w')) = T(\pi(g)(x))$.

Donc $T \in \mathrm{End}_G(\pi)$ et n'est ni nul ni multiple de l'identité de V. Donc dans ce cas $\dim \mathrm{End}_G(\pi) \geq 2$. $\square$

2.2 Le cas des groupes abéliens

Grâce à la proposition 2.1.6 on montre la proposition principale du cas abélien :

Proposition 2.2.1. *Soit* G *un groupe abélien fini et* (π, V) *une représentation irréductible de* G. *Alors,* $\dim(V) = 1$.

Démonstration. Pour $g \in G$, $\pi(g)$ est un G-morphisme car $\forall h \in G$, $\forall v \in V$ $\pi(g)(\pi(h)(v)) = \pi(gh)(v) = \pi(hg)(v) = \pi(h)(\pi(g)(v))$. Donc par la proposition 2.1.6 il existe $\lambda_g \in \mathbb{C}$ tel que $\pi(g) = \lambda_g \cdot \mathrm{Id}_V$. On considère alors un vecteur non nul $v_0 \in V$. Ainsi $< v_0 >$ est un sous-espace de V G-invariant et grâce à l'irréductibilité de (π, V) on conclut $< v_0 >= V$ et donc $\dim(V) = 1$. $\square$

L'étude des représentations irréductibles d'un groupe abélien G se ramène donc à l'étude de l'ensemble $\hat{G}$ des morphismes de G dans $\mathbb{C}^*$. Et on montre aisément en étudiant le cas des $\mathbb{Z}/n\mathbb{Z}$ puis en utilisant la structure des groupes abéliens finis que :

$$G \cong \hat{G}.$$

Remarque 2.2.2. Cet isomorphisme n'est pas canonique.

2.3 L'étude des caractères

2.3.1 Quelques propriétés immédiates d'un caractère χ

Soit (π, V) une représentation de G de cardinal p et χ le caractère associé.

1. $\chi(1) = n$ est le degré de (π, V).
2. $\forall g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$. (Résultat obtenu en diagonalisant $\pi(g)$ et en remarquant que ses valeurs propres sont toutes de module 1 car on a $(\pi(g))^p = \pi(g^p) = \pi(1) = \mathrm{Id}_V$ donc le polynôme caractéristique de $\pi(g)$ divise $X^p - 1$ qui est scindé à racines simples de module 1.)
3. $\forall g \in G, \forall h \in G$, $\chi(ghg^{-1}) = \chi(h)$. (Découle immédiatement du fait que $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.)

Ce dernier résultat montre que $\chi \in \mathcal{H}$.

2.3.2 Résultats sur les liens entre les représentations d'un groupe et les caractères associés

Tout d'abord voici deux propositions importantes dont la réciproque sera montrée par la suite.

Proposition 2.3.1. *Si (π, V) et (π', V') sont deux représentations isomorphes de G alors les caractères associés à ces deux représentations sont identiques.*

Démonstration. Puique (π, V) et (π', V') sont isomorphes il existe un isomorphisme linéaire $T : V \to V'$ tel que $\forall g \in G$, $\pi'(g) = T\pi(g)T^{-1}$. Ainsi $\dim(V) = \dim(V') = n$ donc, après avoir fixé des bases de V et V', $\pi(g)$, $\pi'(g)$ et T peuvent être respectivement vues comme des éléments A_g, B_g et D de $\mathrm{GL}_n(\mathbb{C})$. Et l'égalité réalisée par T signifie que $B_g = DA_gD^{-1}$ et que donc $\chi_{\pi'}(g) = \mathrm{tr}(B_g) = \mathrm{tr}(A_g) = \chi_\pi(g)$ et $\chi_{\pi'} = \chi_\pi$. □

Théorème 2.3.2. *[SIN, Theorem 10.1] La famille des caractères des représentations irréductibles de G forme une famille orthonormale de $(\mathcal{H}, \langle , \rangle)$. En d'autre termes si (π, V) et (π', V') sont deux représentations irréductibles,*

$$\langle \chi_\pi, \chi_{\pi'} \rangle = \begin{cases} 1 & \text{si } (\pi, V) \text{ et } (\pi', V') \text{ sont isomorphes} \\ 0 & \text{sinon} \end{cases}.$$

Ce résultat essentiel n'est pas du tout évident et nécessite de nombreux arguments sur les coefficients des matrices de l'image d'une représentation.

On sait donc maintenant qu'il y a un nombre fini de caractères d'un groupe G (car $\mathcal{H}$ est de dimension finie). On note maintenant $\chi_1, ..., \chi_h$ les caractères irréductibles de G et (π_i, W_i) les représentations irréductibles associées à ces caractères. Si (π, V) est une représentation de dimension finie de G et χ le caractère associé, par totale réductibilité de (π, V) il existe $\alpha_1, ..., \alpha_h$ et un isomorphisme $V \cong W_1^{\alpha_1} \oplus \cdots \oplus W_h^{\alpha_h}$. Ainsi $\chi = \alpha_1\chi_1 + \cdots + \alpha_h\chi_h$. On peut donc maintenant donner le critère d'irréductibilité qui suit ainsi qu'une réciproque à la proposition 2.3.1 :

Proposition 2.3.3 (critère d'irréductibilité)**.** $\langle \chi_\pi, \chi_\pi \rangle = 1$ *si et seulement si* (π, V) *est irréductible.*

Démonstration. Avec les mêmes notations que précédemment on a $V \cong W_1^{\alpha_1} \oplus \cdots \oplus W_h^{\alpha_h}$ et $\chi = \alpha_1\chi_1 + \cdots + \alpha_h\chi_h$ donc par orthogonalité des χ_i, $\langle \chi, \chi \rangle = \sum_{i=1}^h \alpha_i^2$. $\langle \chi, \chi \rangle$ est donc toujours entier et vaut 1 si et seulement si $V \cong W_i$ pour un certain i. $\square$

Proposition 2.3.4. *[SIN, Corollaire 10.4] Deux représentations sont isomorphes si et seulement si leurs caractères sont égaux.*

Démonstration. Le sens direct a été vu en proposition 2.3.1. Pour l'autre sens prenons deux représentations (π, V) et (π', V') de même caractère $\chi = \chi'$. Il existe alors $\alpha_1, ..., \alpha_h, \beta_1, ..., \beta_h$ et deux isomorphismes $V \cong W_1^{\alpha_1} \oplus \cdots \oplus W_h^{\alpha_h}$ et $V' \cong W_1^{\beta_1} \oplus \cdots \oplus W_h^{\beta_h}$. On a alors $\chi = \alpha_1\chi_1 + \cdots + \alpha_h\chi_h$ et $\chi' = \beta_1\chi_1 + \cdots + \beta_h\chi_h$. Et par orthogonalité des χ_i on obtient $\forall i \quad \alpha_i = \beta_i$ donc $V \cong V'$, d'où le résultat. $\square$

D'après cette proposition on peut donc choisir, de façon équivalente, d'étudier les représentations ou les caractères d'un groupe fini.

Enfin voici un résultat un peu plus compliqué mais qui utilise aussi les décompositions utilisées ci-avant :

Proposition 2.3.5. *[JPS, p91] Soient* (π, V) *et* (τ, W) *deux représentations de* G *de caractères* χ_V *et* χ_W*. Alors*

$$\dim(\mathrm{Hom}_G(V, W)) = \langle \chi_V, \chi_W \rangle.$$

2.3.3 Le théorème fondamental de la théorie des caractères

Théorème 2.3.6. *[SIN, Proposition 11.5] L'ensemble des caractères irréductibles de* G *forme une base orthonormale de* $(\mathcal{H}, \langle , \rangle)$*.*

Ce théorème fondamental montre qu'il y a donc exactement autant de caractères irréductibles (ou de représentations irréductibles non-isomorphes) de G que de classes de conjugaison dans G.

2.3.4 Tables de caractères

Le but est maintenant de construire une table donnant l'ensemble des caractères d'un groupe G. On la présentera sous la forme suivante :

	$r_1 = 1$ $g_1 = 1$	$r_2 =$ $g_2 =$	... ...	$r_h =$ $g_h =$
χ_1	$n_1 = 1$	1	...	1
χ_2	n_2	$\chi_2(g_2)$	...	$\chi_2(g_h)$
...	...	...	...	...
χ_h	n_h	$\chi_h(g_2)$	...	$\chi_h(g_h)$

Dans cette table, g_i est un représentant de la i-ème classe de conjugaison de G, r_i est le nombre d'éléments de la i-ème classe de conjugaison et n_i correspond au degré de la représentation irréductible associée à χ_i. On a choisi ici pour χ_1 le caractère de la représentation triviale de G sur $V = \mathbb{C}$ donnée par $\pi(g) = \mathrm{Id}_{\mathbb{C}}$ $\forall g \in G$.

Pour construire ces tables de caractère voici différentes propriétés utiles :

1. Une représentation (π, V) est irréductible si et seulement si $\langle \chi_\pi, \chi_\pi \rangle = 1$ (Proposition 2.3.3).
2. $\sum_{i=1}^h n_i^2 = |G|$. ([SIN, Proposition 12.1])
3. $\forall i \in [1...h]$, $n_i||G|$. ([SIN, Proposition 12.1])
4. Soit $i, j \in [1...h]$. Alors $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ soit $\sum_{t \in G} \chi_i(t)\overline{\chi_j(t)} = \delta_{ij}|G|$. (D'après le théorème 2.3.2.)
5. Soient $t, s \in G$ non conjugués, alors $\sum_{i=1}^h \chi_i(s)\overline{\chi_i(t)} = 0$. (En particulier si $1 \neq s \in G$ on a $\sum_{i=1}^h n_i\chi_i(s) = 0$.) ([SIN, Théorème 10.5])

Cette dernière propriété peut être vue comme l'othogonalité des colonnes de la table de caractères.

2.3.5 Construction de caractères d'un groupe à partir de ceux d'un sous-groupe et réciproquement

Soient G un groupe fini et H un sous-groupe de G. A partir d'un caractère irréductible χ de G on obtient simplement un caractère $\chi_{|H}$ de H en restreignant χ à H, mais ce dernier n'est pas forcément irréductible. En revanche dans tous les cas par le théorème de Maschke il s'écrit sous la forme $\chi_{|H} = d_1\psi_1 + \cdots + d_k\psi_k$, où $\psi_1, \psi_2, ..., \psi_k$ sont les caractères irréductibles de H.

Théorème 2.3.7. *[SIN, Theorème 13.4]. Avec les notations ci-dessus on a l'inégalité suivante :*

$$\sum_{i=1}^{k} d_i^2 \leq [G : H],$$

avec égalité si et seulement si $\chi(g) = 0 \ \forall g \notin H$.

Ce résultat est particulièrement intéressant en pratique dans le cas d'un sous-groupe d'indice 2.

Maintenant voyons comment construire une représentation de G à partir d'une représentation d'un sous-groupe. Soient H un sous-groupe de G et (π, V) une représentation de H. On définit d'abord

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

qui est un espace vectoriel sur $\mathbb{C}$, puis le morphisme π^G de G dans $\mathrm{GL}(V^G)$ par :

$$(\pi^G(g)f)(x) = f(xg).$$

On obtient alors une représentation (π^G, V^G) de G qui est la représentation induite de (π, V) sur G. Le degré de cette représentation induite est $([G : H] \times \dim(V))$.

Et pour savoir à partir d'une représentation irréductible de H si la représentation induite sur G est aussi irréductible, dans le cas où H est un sous-groupe distingué de G on a le théorème suivant :

Théorème 2.3.8. *[PRA, Corollaire 1.18] Supposons que H est un sous-groupe distingué de G. Alors (π^G, V^G) est irréductible si et seulement si $\forall x \notin H$, $({}^x\pi, V)$ n'est pas isomorphe à (π, V), où $({}^x\pi, V)$ est la représentation de H sur V définie par ${}^x\pi(h) = \pi(x^{-1}hx)$.*

Pour finir voici un théorème important qui nous servira plus tard :

Proposition 2.3.9. *[PRA, Réciprocité de Frobenius p2] Soit (τ, U) une représentation de G et (π, V) une représentation de H alors on a un isomorphisme entre $\mathrm{Hom}_G(\tau, \pi^G)$ et $\mathrm{Hom}_H(\tau_H, \pi)$, où (τ_H, U) est la représentation de H obtenue en restreignant le morphisme $\tau : G \to \mathrm{GL}(U)$ à H.*

2.3.6 Autres moyens de construire les caractères d'un groupe

On va commencer par définir quelques notions sur le produit tensoriel de deux représentations, puis nous verrons que grâce à cela on peut construire facilement de nouveaux caractères d'un groupe à partir de ceux déjà connus.

Soient V et V' deux espaces vectoriels. On note $V \otimes V'$ le produit tensoriel de V et V'. On peut voir $V \otimes V'$ comme $= \{\sum_{i=1}^{r} v_i \otimes v_i' | v_i \in V, v_i' \in V', r \in \mathbb{N}\}$, avec les propriétés suivantes :

1. $(\sum_{i=1}^r v_i \otimes v_i') + (\sum_{i=1}^s w_i \otimes w_i') = v_1 \otimes v_1' + \cdots + v_r \otimes v_r' + w_1 \otimes w_1' + \cdots + w_1 \otimes w_s'$.
2. $(v_1 + v_2) \otimes v' = v_1 \otimes v' + v_2 \otimes v'$ et $v \otimes (v_1' + v_2') = v \otimes v_1' + v \otimes v_2'$
3. $\lambda(\sum_{i=1}^r v_i \otimes v_i') = \sum_{i=1}^r \lambda v_i \otimes v_i' = \sum_{i=1}^r v_i \otimes \lambda v_i'$.

On constate tout d'abord que si $\{e_1, ..., e_n\}$ et $\{e_1', ..., e_m'\}$ sont respectivement des bases de V et V' alors $\{e_i \otimes e_j' | 1 \leq i \leq n, 1 \leq j \leq m\}$ est une base de $V \otimes V'$.

Si (π, V) et (π', V') sont deux représentations de G on définit la représentation $(\pi \otimes \pi', V \otimes V')$ de G par

$$(\pi \otimes \pi')(g)(\sum_i v_i \otimes v_i') = \sum_i \pi(g)(v_i) \otimes \pi'(g)(v_i').$$

Pour finir on note θ l'automorphisme de $V \otimes V$ défini par $\theta(e_i \otimes e_j) = e_j \otimes e_i$. On constate alors que $\theta^2 = \mathrm{Id}_{V \otimes V}$. Et par somme directe des espaces propres on a $V \otimes V = \mathrm{Sym}^2(V) \oplus \Lambda^2(V)$ où

$$\mathrm{Sym}^2(V) = \{x \in V \otimes V | \theta(x) = x\}$$
$$\Lambda^2(V) = \{x \in V \otimes V | \theta(x) = -x\}$$

On a alors les deux propositions suivantes, importantes pour construire les caractères d'un groupe.

Proposition 2.3.10. *[SIN, Proposition 9.9] Si χ_1 et χ_2 sont les caractères de deux représentations (π, V) et (π', V') de G alors le caractère χ associé à $(\pi \otimes \pi', V \otimes V')$ vérifie $\forall g \in G$ $\chi(g) = \chi_1(g)\chi_2(g)$.*

Remarque 2.3.11. Le résultat à retenir est que le produit de deux caractères est un caractère.

Proposition 2.3.12. *[SIN, Theorème 13.2] Soit (π, V) une représentation de G de caractère χ. Alors les espaces $\mathrm{Sym}^2(V)$ et $\Lambda^2(V)$ sont G-invariants pour la représentation $(\pi \otimes \pi, V \otimes V)$ et si on note χ_S et χ_A les caractères des représentations $((\pi \otimes \pi)_{|Sym^2(V)}, Sym^2(V))$ et $((\pi \otimes \pi)_{|\Lambda^2(V)}, \Lambda^2(V))$ respectivement, alors on a $\forall g \in G$*

$$\chi_S(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$
$$\chi_A(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

Remarque 2.3.13. Ces propositions donnent des moyens de construire de nouveaux caractères de G à partir de caractères déja connus, mais en aucun cas ils ne donnent le moindre résultat concernant l'irréductibilité ou non ce ces derniers.

3 Exemples de tables de caractères

3.1 $\mathbb{Z}/n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien. Les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ sont donc toutes de degré 1. Si on note ω_n le complexe $e^{\frac{2i\pi}{n}}$ les caractères de $\mathbb{Z}/n\mathbb{Z}$, au nombre de n, sont les fonctions χ_r suivantes :

$$\chi_r(s) = \omega_n^{rs} \text{ pour } s \in \mathbb{Z}/n\mathbb{Z} \text{ et } r \in \{0, ..., n-1\}.$$

3.2 $\mathfrak{S}_3$

$$\mathfrak{S}_3 = \{1, (12), (23), (13), (123), (132)\}.$$

$\mathfrak{S}_3$ possède 3 caractères car c'est son nombre de classes de conjugaison. Il y a tout d'abord le caractère trivial χ_1. Ensuite on a le morphisme χ_2 donné par la signature des éléments de $\mathfrak{S}_3$. Puis par la formule $\sum_{i=1}^{h} n_i^2 = |G|$ on obtient que le troisième caractère χ_3 est tel que $n_3 = 2$. On obtient donc pour l'instant la table de caractères suivante.

	$r_1 = 1$ $g_1 = 1$	$r_2 = 3$ $g_2 = (12)$	$r_3 = 2$ $g_3 = (123)$
χ_1	$n_1 = 1$	1	1
χ_2	$n_2 = 1$	-1	1
χ_3	$n_3 = 2$	a	b

Pour avoir a et b il suffit d'utiliser l'orthogonalité des colonnes de la table de caractères. Ainsi on obtient $a = 0$ et $b = -1$. On peut remarquer que χ_3 correspond à la représentation irréductible de $\mathfrak{S}_3$ de degré 2 décrite dans l'exemple 1.2.7. Donc la table de caractères de $\mathfrak{S}_3$ est :

	$r_1 = 1$ $g_1 = 1$	$r_2 = 3$ $g_2 = (12)$	$r_3 = 2$ $g_3 = (123)$
χ_1	$n_1 = 1$	1	1
χ_2	$n_2 = 1$	-1	1
χ_3	$n_3 = 2$	0	-1

3.3 D_4, le groupe des symétries du carré.

$$D_4 = \{r, s | r^4 = 1 = s^2, rs = sr^{-1}\}.$$

D_4 a cinq classes de conjugaison qui sont $\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}$ et $\{sr, sr^3\}$. Il y a donc 5 représentations irréductibles de D_4. De plus la formule $\sum_{i=1}^h n_i^2 = |G|$ nous indique que 4 d'entre elles sont de degré 1 et une de degré 2. χ_1 est le caractère trivial. On a donc pour l'instant une table de caractères de cette forme :

	$r_1 = 1$ $g_1 = 1$	$r_2 = 1$ $g_2 = r^2$	$r_3 = 2$ $g_3 = r$	$r_4 = 2$ $g_4 = s$	$r_5 = 2$ $g_5 = sr$
χ_1	$n_1 = 1$	1	1	1	1
χ_2	$n_2 = 1$	x_1	x_2	x_3	x_4
χ_3	$n_3 = 1$	y_1	y_2	y_3	y_4
χ_4	$n_3 = 1$	z_1	z_2	z_3	z_4
χ_5	$n_3 = 2$	a	b	c	d

Pour trouver les x_i, y_i et z_i en raisonnant sur l'ordre des éléments de D_4 on remarque tout d'abord que si $i \neq 2$ ils sont égaux à 1 ou -1 et pour $i = 2$ ils valent 1, -1, i ou $-i$. De plus les 3 dernières classes de conjugaison de D_4 sont stables par multiplication à droite par r^2. Donc $x_1 = y_1 = z_1 = 1$. Ensuite $s \cdot r = sr$ donc $x_2 x_3 = x_4$, $y_2 y_3 = y_4$ et $z_2 z_3 = z_4$. Ce qui implique que même pour $i = 2$ x_i, y_i et z_i valent -1 ou 1. De nouveau en utilisant $x_2 x_3 = x_4$ et le caractère non trivial de χ_2 on trouve que exactement deux des x_i valent -1. De même pour les y_i et les z_i. Ce qui pour l'instant donne la table de caractères :

	$r_1 = 1$ $g_1 = 1$	$r_2 = 1$ $g_2 = r^2$	$r_3 = 2$ $g_3 = r$	$r_4 = 2$ $g_4 = s$	$r_5 = 2$ $g_5 = sr$
χ_1	$n_1 = 1$	1	1	1	1
χ_2	$n_2 = 1$	1	1	-1	-1
χ_3	$n_3 = 1$	1	-1	1	-1
χ_4	$n_3 = 1$	1	-1	-1	1
χ_5	$n_3 = 2$	a	b	c	d

Puis par othogonalité des colonnes on obtient $a = -2$ et $b = c = d = 0$. Donc finalement la table de caractères de D_4 est la suivante :

	$r_1 = 1$ $g_1 = 1$	$r_2 = 1$ $g_2 = r^2$	$r_3 = 2$ $g_3 = r$	$r_4 = 2$ $g_4 = s$	$r_5 = 2$ $g_5 = sr$
χ_1	$n_1 = 1$	1	1	1	1
χ_2	$n_2 = 1$	1	1	-1	-1
χ_3	$n_3 = 1$	1	-1	1	-1
χ_4	$n_3 = 1$	1	-1	-1	1
χ_5	$n_3 = 2$	-2	0	0	0

Remarque 3.3.1. D_4 est le groupe des symétries d'un carré. On voyant ce carré dans $\mathbb{R}^2$ on obtient donc une représentation naturelle de D_4 sur $\mathbb{R}^2$. Puis on peut

étendre cette représentation sur $\mathbb{C}^2$. On obtient ainsi l'unique représentation irréductible de D_4 de degré 2 qui est associée à χ_5.

3.4 $\mathfrak{S}_5$

$\mathfrak{S}_5$ a 120 éléments, je ne vais donc pas donner ses éléments de façon exhaustive. En revanche je peux donner un représentant de chacune de ses 7 classes de conjugaison. Ces classes sont définies par la structure des cycles de ses éléments. On a donc les classes suivantes avec leur cardinal :

r_i	1	10	20	15	30	20	24
g_i	1	(12)	(123)	(12)(34)	(1234)	(12)(345)	(12345)

On va maintenant construire chacun des 7 caractères de $\mathfrak{S}_5$:

1. Tout d'abord comme pour tous les $\mathfrak{S}_n$ on a les caractères χ_1 et χ_2 correspondant au caractère trivial et à la signature des éléments de $\mathfrak{S}_n$.

r_i	1	10	20	15	30	20	24
g_i	1	(12)	(123)	(12)(34)	(1234)	(12)(345)	(12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1

2. Ensuite on utilise la représentation irréductible de $\mathfrak{S}_n$ de degré $n-1$ décrite dans l'exemple 1.2.7. Elle est définie sur $Y = \{(x_1, ..., x_5) | \sum x_i = 0\}$ de dimension 4 et dont une base est $(e_1 - e_2, e_2 - e_3, e_3 - e_4, e_4 - e_5)$. L'action des éléments de $\mathfrak{S}_5$ est naturelle. On calcule ainsi l'image des vecteurs de la base précédente de Y par l'action des éléments de $\mathfrak{S}_5$ puis on prend la trace de la matrice associée pour obtenir le caractère χ_3 de $\mathfrak{S}_5$:

   Action de (12) :

$$(e_1 - e_2) \mapsto e_2 - e_1 = -(e_1 - e_2)$$
$$(e_2 - e_3) \mapsto e_1 - e_3 = (e_1 - e_2) + (e_2 - e_3)$$
$$(e_3 - e_4) \mapsto (e_3 - e_4)$$
$$(e_4 - e_5) \mapsto (e_4 - e_5)$$

   d'où la matrice $\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ et $\chi_3((12)) = 2$.

   Action de (123) : On obtient la matrice $\begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ et $\chi_3((123)) = 1$.

Et ainsi de suite on fait de même avec un élément de chaque classe de conjugaison.

r_i	1	10	20	15	30	20	24
g_i	1	(12)	(123)	(12)(34)	(1234)	(12)(345)	(12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1

3. On va maintenant utiliser la proposition 2.3.10 pour construire un nouveau caractère. Celle-ci nous dit que $\chi_4 = \chi_2\chi_3$ est un caractère de $\mathfrak{S}_5$ mais il faut savoir si il est irréductible. Pour cela on utilise le critère d'irréductibilité de la proposition 2.3.3 :

$$\langle \chi_2\chi_3, \chi_2\chi_3 \rangle = \frac{1}{120}((4)^2 + 10(-2)^2 + 20(1)^2 + 20(1)^2 + 24(-1)^2) = 1$$

C'est donc bien un nouveau caractère irréductible de $\mathfrak{S}_5$.

r_i	1	10	20	15	30	20	24
g_i	1	(12)	(123)	(12)(34)	(1234)	(12)(345)	(12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1

4. A l'aide de la proposition 2.3.12 on sait que χ_A défini par $\chi_A(g) = \frac{1}{2}(\chi_3(g)^2 - \chi_3(g^2))$ est un caractère, de plus on remarque par le calcul de $\langle \chi_A, \chi_A \rangle$ qu'il est irréductible. Etant différent de ceux construits jusque là il est notre cinquième caractère irréductible χ_5.

r_i	1	10	20	15	30	20	24
g_i	1	(12)	(123)	(12)(34)	(1234)	(12)(345)	(12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	6	0	0	-2	0	0	1

5. Toujours à partir de χ_3 avec la proposition 2.3.12 on a le caractère χ_S défini par $\chi_S(g) = \frac{1}{2}(\chi_3(g)^2 + \chi_3(g^2))$. Cette fois $\langle \chi_S, \chi_S \rangle = 3$ et χ_S n'est donc pas irréductible. En revanche on sait qu'il existe $m_1, ..., m_7$ tel que $\chi_S =$

$m_1\chi_1+\cdots+m_7\chi_7$ et $m_i = \langle \chi_S, \chi_i\rangle$. Or $\langle \chi_S, \chi_1\rangle = \langle \chi_S, \chi_3\rangle = 1$ et $\langle \chi_S, \chi_2\rangle = \langle \chi_S, \chi_4\rangle = \langle \chi_S, \chi_5\rangle = 0$, donc $\chi_S = \chi_1 + \chi_3 + \chi_6$ (ça peut être χ_7 au lieu de χ_6 mais quitte à échanger les deux cela n'a pas d'importance car on ne les a justement pas encore construits). On vient donc de construire le sixième caractère de $\mathfrak{S}_5$ qui est $\chi_6 = \chi_S - \chi_1 + \chi_3$.

r_i g_i	1 1	10 (12)	20 (123)	15 (12)(34)	30 (1234)	20 (12)(345)	24 (12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	6	0	0	-2	0	0	1
χ_6	5	1	-1	1	-1	1	0
χ_7	a	b	c	d	e	f	g

6. Pour avoir χ_7 soit on utilise l'orthogonalité des colonnes de la table de caractères soit on peut remarquer que $\chi_2\chi_6$ est un nouveau caractère irréductible. Ce qui nous donne enfin la table de caractères complète de $\mathfrak{S}_5$:

r_i g_i	1 1	10 (12)	20 (123)	15 (12)(34)	30 (1234)	20 (12)(345)	24 (12345)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	6	0	0	-2	0	0	1
χ_6	5	1	-1	1	-1	1	0
χ_7	5	-1	-1	1	1	-1	0

4 Le cas de $\mathrm{GL}_2(\mathbb{F}_q)$

Le but de cette partie est de construire l'ensemble des représentations (ou caractères) irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$. Pour cela nous allons commencer par une petite analyse de $\mathbb{F}_q$ et de $\mathrm{GL}_2(\mathbb{F}_q)$. Ensuite nous construirons deux types de représentations irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$, tout d'abord en utilisant directement l'induite à partir d'un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$, ensuite en utilisant la représentation de Weil et l'étude du groupe d'Heisenberg. Nous verrons alors que nous obtenons toutes les représentations irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$ par ces deux méthodes. Dans toute la partie on prendra $q = p^k$ avec p un nombre premier impair et k un entier strictement positif.

4.1 Propriétés importantes de $\mathbb{F}_q$ et de son extension quadratique $\mathbb{F}_{q^2}$

Tout d'abord on rappelle que pour toute puissance p^k d'un nombre premier p il existe un unique corps fini d'ordre p^k, à isomorphisme près, que l'on note $\mathbb{F}_q$ avec $q = p^k$. Ainsi concrètement $\mathbb{F}_q$ est l'ensemble des racines du polynôme $X^q - X$ de $\overline{\mathbb{F}_p}[X]$ où $\overline{\mathbb{F}_p}$ est une clôture algébrique de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Théorème 4.1.1. *$\mathbb{F}_q^*$ est cyclique donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Démonstration. $\mathbb{F}_q^*$ est un groupe abélien donc il existe $n_1, ..., n_s$ tels que $n_1|n_2|...|n_s$ et $\mathbb{F}_q^* \cong \mathbb{Z}/n_1\mathbb{Z} \times .... \times \mathbb{Z}/n_s\mathbb{Z}$. Soit d un diviseur de $q-1 = |\mathbb{F}_q^*|$. D'après cette décomposition le nombre de solutions de $X^d - 1 = 0$ dans $\mathbb{F}_q^*$ est $\text{pgcd}(n_1, d) \times \text{pgcd}(n_2, d) \times ... \times \text{pgcd}(n_s, d)$. Prenons alors le cas $d = n_1$ (qui est bien un diviseur de $|\mathbb{F}_q^*|$). Cela donne n_1^s racines de $X^{n_1} - 1 = 0$ dans $\mathbb{F}_q^*$, or ce polynôme est de degré n_1 donc il a au plus n_1 racines, ce qui implique que $s = 1$ et $\mathbb{F}_q^* = \mathbb{Z}/n_1\mathbb{Z} = \mathbb{Z}/(q-1)\mathbb{Z}$ qui est cyclique. □

$\mathbb{F}_{q^2}$ est une extension quadratique de $\mathbb{F}_q$. $\mathbb{F}_{q^2}$ peut alors être vu comme un $\mathbb{F}_q$-espace vectoriel de dimension 2. Pour $x \in \mathbb{F}_{q^2}$ on définit l'application linéaire $m_x : y \in \mathbb{F}_{q^2} \mapsto xy$ ainsi que les applications trace et norme de $\mathbb{F}_{q^2}$ dans $\mathbb{F}_q$ comme suit : $\text{tr}(x) = \text{tr}(m_x)$ et $N(x) = \det(m_x)$. De plus on définit l'application $F : x \mapsto x^q$ qui est un automorphisme de corps de $\mathbb{F}_{q^2}$ (automorphisme de Frobenius), on note aussi $F(x) = \bar{x}$. On a alors les propriétés suivantes :

1. $x = \bar{x}$ si et seulement si $x \in \mathbb{F}_q$.
2. $\text{tr}(x) = x + \bar{x}$
3. $\text{tr}(x + x') = \text{tr}(x) + \text{tr}(x')$.
4. $N(x) = x\bar{x}$.
5. $N(xx') = N(x)N(x')$.
6. Soit $x \in \mathbb{F}_q$, alors le nombre d'éléments $y \in \mathbb{F}_{q^2}$ tels que $N(y) = x$ est $q+1$ si $x \neq 0$ et 1 sinon (ce qui montre en particulier que $N : \mathbb{F}_{q^2} \to \mathbb{F}_q$ est surjective).

Les propriétés 1 à 5 sont immédiates en revanche voici la démonstration du 6 :

Démonstration. D'après la propriété 4 on a $N(y) = y^{q+1}$. Si $x = 0$ alors il est clair que $N(y) = 0$ si et seulement si $y = 0$. On fixe maintenant $x \in \mathbb{F}_q^*$ et on considère le polynôme $X^{q+1} - x$ dans $\overline{\mathbb{F}_p}[X]$. $(X^{q+1} - x)' = X^q$ or 0 n'est pas racine de $X^{q+1} - x$ donc ce dernier n'a pas de racine double et a donc exactement $q+1$ racines distinctes dans $\overline{\mathbb{F}_p}$ que l'on note $\alpha_1, ..., \alpha_{q+1}$, ces dernières étant non nulles. $(\alpha_i)^{q^2} = (\alpha_i^q)^q = (\alpha_i^{-1}x)^q = (\alpha_i^q)^{-1}x^q = (x\alpha_i^{-1})^{-1}x = \alpha_i$. Donc les α_i sont tous dans $\mathbb{F}_{q^2}$, ce qui montre que l'équation $N(y) = x$ (d'inconnue y) a exactement $q+1$ solutions dans $\mathbb{F}_{q^2}$. □

Si $(G,+)$ est un groupe abélien fini, l'ensemble des morphismes de G dans $\mathbb{C}^*$ est exactement l'ensemble des caractères irréductibles de G (car les représentations irréductibles d'un groupe abélien sont de degré 1). Un caractère de $(G,+)$ abélien est donc simplement un morphisme de $(G,+)$ dans $\mathbb{C}^*$, et ces caractères sont au nombre de $|G|$.

Comme on l'a fait ci-dessus on définit l'application $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ à partir de la multiplication $m_x : y \in \mathbb{F}_q \mapsto xy$ où $x \in \mathbb{F}_q$ et où $\mathbb{F}_q$ est vu comme un $\mathbb{F}_p$-espace vectoriel de dimension k.

Soit $\psi^0 : \mathbb{F}_p \to \mathbb{C}^*$ un caractère non-trivial de $(\mathbb{F}_p,+)$. Alors $\psi : \mathbb{F}_q \to \mathbb{C}^*$ défini par $\psi(x) = \psi^0(\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x))$ est un caractère non-trivial de $(\mathbb{F}_q,+)$. Puis pour $x' \in \mathbb{F}_q$ on définit $\psi_{x'} : \mathbb{F}_q \to \mathbb{C}^*$ par $\psi_{x'}(x) = \psi(x'x)$. On a alors les deux propositions suivantes :

Proposition 4.1.2. *[PRA, Proposition B.11] L'application $x' \mapsto \psi_{x'}$ est un isomorphisme de $\mathbb{F}_q$ sur $\widehat{\mathbb{F}_q}$.*

Proposition 4.1.3. *L'application $x \mapsto (y \mapsto \psi(\mathrm{tr}(\bar{x}y)))$ est un isomorphisme de $\mathbb{F}_{q^2}$ sur $\widehat{\mathbb{F}_{q^2}}$.*

Remarque 4.1.4. Ce dernier résultat se montre en appliquant la proposition 4.1.2 à $q = p^{2k}$.

4.2 Analyse de $\mathrm{GL}_2(\mathbb{F}_q)$

Commençons par calculer le cardinal de $\mathrm{GL}_2(\mathbb{F}_q)$. Un élément de $\mathrm{GL}_2(\mathbb{F}_q)$ peut être vu comme un couple de deux vecteurs indépendants d'un $\mathbb{F}_q$-espace vectoriel de dimension 2. Pour choisir le premier vecteur il y a donc (q^2-1) possibilités (il suffit d'un vecteur non nul) et pour le suivant (q^2-q) car il ne doit pas être égal à l'un des q vecteurs liés avec le premier choisi. D'où le résultat :

$$|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q).$$

Ensuite nous savons qu'il y a autant de caractères irréductibles que de classes de conjugaison. Nous allons donc nous intéresser à ces classes de conjugaison dans $\mathrm{GL}_2(\mathbb{F}_q)$ qui sont donc des classes de matrices semblables. Pour cela on utilise le polynôme caractéristique des éléments de $\mathrm{GL}_2(\mathbb{F}_q)$. Soit $A \in \mathrm{GL}_2(\mathbb{F}_q)$ et P son polynôme caractéristique. Quatre cas se présentent :

1. P est scindé à racines simples sur $\mathbb{F}_q$, dans ce cas A est semblable à une matrice de la forme $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ avec $\lambda_1 \neq \lambda_2$ et $\lambda_i \in \mathbb{F}_q^*$. Il y a $\frac{(q-1)(q-2)}{2}$ telles classes de conjugaison.

2. P est scindé sur $\mathbb{F}_q$ avec une racine double et A diagonalisable, dans ce cas A est semblable à une matrice de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{F}_q^*$. Il y a $(q-1)$ telles classes de conjugaison.
3. P est scindé sur $\mathbb{F}_q$ avec une racine double et A non diagonalisable, dans ce cas A est semblable à une matrice de la forme $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{F}_q^*$. Il y a $(q-1)$ telles classes de conjugaison.
4. P est irréductible sur $\mathbb{F}_q$, dans ce cas A est semblable à une matrice de la forme $\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix}$ avec $P(X) = X^2 - a_1X + a_0$ un polynôme irréductible dans $\mathbb{F}_q[X]$. Ce cas là est moins évident que les trois précédents, voici donc une explication détaillée : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{GL}_2(\mathbb{F}_q)$ de polynôme caractéristique irréductible $X^2 - (a+b)X + (ad - bc)$. Ceci implique que $c \neq 0$ sinon $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ serait triangulaire et $X^2 - (a+b)X + (ad-bc)$ scindé. Puis le calcul suivant montre le résultat : $\begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}^{-1} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & -a/c \\ 0 & 1/c \end{pmatrix} \times \begin{pmatrix} a & a^2 - bc \\ c & ac - dc \end{pmatrix} = \begin{pmatrix} 0 & -(ad-bc) \\ 1 & a+b \end{pmatrix}$. Il y a $\frac{(q^2-q)}{2}$ polynômes irréductibles unitaires dans $\mathbb{F}_q[X]$ donc $\frac{(q^2-q)}{2}$ classes de conjugaison de ce type.

Il y a donc au total $(q-1) + (q-1) + \frac{(q^2-q)}{2} + \frac{(q-1)(q-2)}{2}$ représentations irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$.

Maintenant définissons trois sous-groupes de $\mathrm{GL}_2(\mathbb{F}_q)$ qui seront utilisés par la suite. On notera D le sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$ contenant les matrices diagonales, T celui des matrices triangulaires supérieures et U celui des matrices triangulaires supérieures avec des 1 sur la diagonale.

Enfin pour finir avec cette petite analyse de $\mathrm{GL}_2(\mathbb{F}_q)$ voyons ce que l'on appelle la décomposition de Bruhat de $\mathrm{GL}_2(\mathbb{F}_q)$:

Proposition 4.2.1 (décomposition de Bruhat)**.** *En notant* $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *on a le résultat suivant :*

$$\mathrm{GL}_2(\mathbb{F}_q) = T \sqcup TwT$$

où l'union est disjointe.

Démonstration. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{GL}_2(\mathbb{F}_q)$. Soit $c = 0$ et dans ce cas $A \in T$ soit $c \neq 0$ et dans ce cas $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} -c & -d \\ 0 & b - ad/c \end{pmatrix} \in TwT$. □

Remarque 4.2.2. De façon générale on a

$$\mathrm{GL}_n(k) = \bigsqcup_{\omega \in \mathfrak{S}_n} TA_\omega T,$$

où T est l'ensemble des matrices triangulaires supérieures et A_ω est la matrice de permutation associée à ω. Notre "ω" ci-dessus n'est pas une matrice de permutation mais ça ne change rien car $\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Pour finir voici un dernier résultat concernant $\mathrm{SL}_2(\mathbb{F}_q)$. Pour $a \in \mathbb{F}_q^*$ et $c \in \mathbb{F}_q$ on note : $t(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $u(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ et $\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Proposition 4.2.3. *Les matrices t(a), u(c) et w engendrent* $\mathrm{SL}_2(\mathbb{F}_q)$.

Démonstration. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$. Si $b = 0$ alors $d = a^{-1}$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = t(a)u(ac)$, sinon $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = u(\frac{d}{b})\omega u(ab)t(b^{-1})$. □

4.3 Les représentations induites de $\mathrm{GL}_2(\mathbb{F}_q)$

4.3.1 Construction de ces représentations

Le principe pour construire ces représentations va être de construire un caractère sur T à partir d'un caractère de $\mathbb{F}_q^*$ pour induire alors une représentation sur $\mathrm{GL}_2(\mathbb{F}_q)$.

Pour commencer prenons deux morphismes de groupe χ_1 et χ_2 de $\mathbb{F}_{q^2}^*$ dans $\mathbb{C}^*$. Ensuite on définit le morphisme de groupe χ de T dans $\mathbb{C}^*$ comme suit :

$$\chi \begin{pmatrix} y_1 & a \\ 0 & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2).$$

On vérifie aisément que c'est un morphisme et qu'il est donc associé à une représentation de T de degré 1.

On note $I(\chi_1, \chi_2)$ la représentation induite sur $\mathrm{GL}_2(\mathbb{F}_q)$ de la représentation de T associée à χ. Le cardinal de T est $(q-1)(q-1)q$ donc l'indice de T dans $\mathrm{GL}_2(\mathbb{F}_q)$ est $q+1$, ce qui est alors aussi le degré de ces représentations induites.

4.3.2 Irréductibilité de ces représentations

Maintenant il s'agit de voir si ces représentations sont irréductibles et, si ce n'est pas le cas, de trouver quelles sont les représentations irréductibles qui les composent. Pour cela voici une proposition et un théorème importants :

Proposition 4.3.1. *[PRA, Proposition 2.6] Soient χ_1, χ_2, μ_1 et μ_2 des caractères irréductibles de $\mathbb{F}_q^*$. Alors*

$$\dim \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) = e_1 + e_w,$$

où

$$e_1 = \begin{cases} 1 & si\ \chi_1 = \mu_1\ et\ \chi_2 = \mu_2 \\ 0 & sinon \end{cases}$$

et

$$e_w = \begin{cases} 1 & si\ \chi_1 = \mu_2\ et\ \chi_2 = \mu_1 \\ 0 & sinon \end{cases}$$

Théorème 4.3.2. *Soient χ_1, χ_2, μ_1 et μ_2 des caractères irréductibles de $\mathbb{F}_q^*$. Alors, si $\chi_1 \neq \chi_2$, $I(\chi_1, \chi_2)$ est une représentation irréductible de degré $q+1$ de $\mathrm{GL}_2(\mathbb{F}_q)$. Sinon c'est la somme directe d'une représentation irréductible de degré 1 et d'une autre de degré q. De plus si $\chi_1 \neq \mu_1$ les représentations irréductibles de degré 1 et q qui composent $I(\chi_1, \chi_1)$ et $I(\mu_1, \mu_1)$ sont deux à deux non isomorphes. Et dans le cas où $\chi_1 \neq \chi_2$ et $\mu_1 \neq \mu_2$ on a :*

$$(I(\chi_1, \chi_2) \cong I(\mu_1, \mu_2)) \Longleftrightarrow \begin{cases} \chi_1 = \mu_1\ et\ \chi_2 = \mu_2 \\ ou \\ \chi_1 = \mu_2\ et\ \chi_2 = \mu_1 \end{cases}$$

Démonstration. Par la proposition 4.3.1 dans le cas $\chi_1 = \mu_1$ et $\chi_2 = \mu_2$ on a

$$\dim \mathrm{End}_{\mathrm{GL}_2(\mathbb{F}_q)}(I(\chi_1, \chi_2)) = \begin{cases} 1 \text{ si } \chi_1 \neq \chi_2 \\ 2 \text{ si } \chi_1 = \chi_2 \end{cases}$$

Or si (π, V) est une représentation d'un groupe G (de caractère ψ) c'est une somme directe de représentations irréductibles $\pi_1, ..., \pi_h$ (de caractères $\psi_1, ..., \psi_h$) avec multiplicités $n_1, ..., n_h$ respectivement et d'après la proposition 2.3.5 $\dim \mathrm{End}_G(\pi) = \langle \psi, \psi \rangle = \langle n_1\psi_1 + \cdots + n_h\psi_h, n_1\psi_1 + \cdots + n_h\psi_h \rangle = \sum_{i=1}^h n_i^2$. Donc, si $\chi_1 \neq \chi_2$ $I(\chi_1, \chi_2)$ est irréductible, sinon on a $\sum_{i=1}^h n_i^2 = 2$ donc $I(\chi_1, \chi_2)$ est la somme directe de deux représentations irréductibles non isomorphes.

Regardons le cas où $\chi_1 = \chi_2$. Soit $f : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{C}$ définie par $f(g) = \chi_1(\det(g))$. Pour $t \in T$ et $g \in G$ on a $f(tg) = \chi_1(\det(t))\chi_1(\det(g)) = \chi_1(t)f(g)$.

Donc f appartient à l'espace vectoriel sous-jacent à la représentation $I(\chi_1, \chi_1)$. De plus $(g \cdot f)(x) = f(xg) = \chi_1(\det(g))\chi_1(\det(x)) = \chi_1(\det(g))f(x)$. Ce qui montre que la droite engendrée par f est $\mathrm{GL}_2(\mathbb{F}_q)$-invariante pour la représentation $I(\chi_1, \chi_1)$ et donc que cette dernière contient une représentation irréductible de degré 1. L'autre composante irréductible de $I(\chi_1, \chi_1)$ est donc de dimension q. Puis si $\chi_1 \neq \mu_1$ $\dim \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{F}_q)}(I(\chi_1, \chi_1), I(\mu_1, \mu_1)) = 0$ donc les représentations irréductibles de degré 1 et q qui composent $I(\chi_1, \chi_1)$ et $I(\mu_1, \mu_1)$ sont deux à deux non isomorphes.

Pour la fin du théorème, si $\chi_1 \neq \chi_2$ et $\mu_1 \neq \mu_2$ alors $I(\chi_1, \chi_2)$ et $I(\mu_1, \mu_2)$ sont irréductibles et par la proposition 4.3.1 $\dim \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) = 1$ si et seulement si $\chi_1 = \mu_1$ et $\chi_2 = \mu_2$ ou $\chi_1 = \mu_2$ et $\chi_2 = \mu_2$, d'où le résultat. $\square$

On vient de construire de nombreuses représentations irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$ dont voici le bilan :

1. Si $\chi_1 \neq \chi_2$, $I(\chi_1, \chi_2)$ est irréductible et isomorphe à $I(\chi_2, \chi_1)$, or il y a $|\mathbb{F}_q^*| = (q-1)$ caractères de $\mathbb{F}_q^*$ (car c'est un groupe abélien) donc cela fait $\frac{(q-1)(q-2)}{2}$ représentations irréductibles, deux à deux non isomorphes, de $\mathrm{GL}_2(\mathbb{F}_q)$ de degré $q+1$.
2. Si $\chi_1 \in \mathbb{F}_q^*$, $I(\chi_1, \chi_1)$ apporte une représentation irréductible de degré 1 et une de degré q de $\mathrm{GL}_2(\mathbb{F}_q)$. Cela fait donc $q-1$ représentations irréductibles, deux à deux non isomorphes, de $\mathrm{GL}_2(\mathbb{F}_q)$ de degré 1 et $q-1$ représentations irréductibles, deux à deux non isomorphes, de $\mathrm{GL}_2(\mathbb{F}_q)$ de degré q.

Ce qui fait donc un total de $(q-1) + (q-1) + \frac{(q-1)(q-2)}{2}$ représentations irréductibles, deux à deux non isomorphes, de $\mathrm{GL}_2(\mathbb{F}_q)$ construites dans cette partie.

4.4 Les représentations cuspidales de $\mathrm{GL}_2(\mathbb{F}_q)$

Dans cette partie nous allons voir comment construire les $\frac{q^2-q}{2}$ représentations irréductibles restantes.

Définition 4.4.1. Une représentation (π, V) de $\mathrm{GL}_2(\mathbb{F}_q)$ est dite cuspidale si $\forall\ \chi_1, \chi_2 \in \widehat{\mathbb{F}_q^*}$

$$\dim \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{F}_q)}(\pi, I(\chi_1, \chi_2)) = 0$$

En d'autres termes c'est une représentation qui ne comprend comme sous-représentation aucune des représentations irréductibles construites dans la partie précédente.

Remarque 4.4.2. Cette définition implique en particulier, par la proposition 2.3.9, que pour tout caractère χ de T tel que $\chi_{|U} \equiv 1$ on a

$$\dim \mathrm{Hom}_T(\pi_T, \chi) = 0.$$

4.5 Caractérisation et degré des représentations cuspidales de $\mathrm{GL}_2(\mathbb{F}_q)$

On va commencer par définir ce qu'est la représentation duale d'une représentation :

Définition 4.5.1. Soit (π, V) une représentation de G. On définit (π^*, V^*) la représentation duale de (π, V) par $\pi^*(g) = \pi(g^{-1})^*$ où pour $f \in V^*$ et $v \in V$, $(\pi(g^{-1})^*)(f)(v) = f(\pi(g^{-1})(v))$.

Voici alors une caractérisation des représentations cuspidales à l'aide des représentations duales :

Proposition 4.5.2. *Soit (π, V) une représentation de $\mathrm{GL}_2(\mathbb{F}_q)$. Alors (π, V) est cuspidale si et seulement si il n'existe aucun vecteur non-nul $f \in V^*$ tel que*

$$\forall u \in U, \ \pi^*(u)f = f$$

Démonstration. Supposons que (π, V) n'est pas cuspidale. Par la remarque 4.4.2 il existe un élément non-nul $\xi \in \mathrm{Hom}_T(\pi, \chi)$ pour un certain $\chi : T \to \mathbb{C}^*$ tel que $\chi_{|U} \equiv 1$. $(\chi, \mathbb{C})$ étant une représentation de T, ξ est alors un élément de $\mathrm{Hom}(V, \mathbb{C})$ donc peut être vu comme un élément de V^*. De plus $\forall u \in U, v \in V$ on a

$$(\pi^*(u)\xi)(v) = \xi(\pi(u^{-1})v) = \chi(u^{-1})\xi(v) = \xi(v),$$

ce qui montre bien que $\pi^*(u)\xi = \xi$.

Réciproquement supposons que $V^{*U} = \{\xi \in V^* | \pi^*(u)\xi = \xi \quad \forall u \in U\}$ est non vide. V^{*U} est stable par l'action de D (car $dUd^{-1} = U$ pour tout $d \in S$). Ainsi $((\pi^*_{|D})_{V^{*U}}, V^{*U})$ est une représentation de D qui est un groupe abélien. On peut donc décomposer V^{*U} sous la forme

$$V^{*U} = \bigoplus_{\chi \in \widehat{D}} V^{*U}_\chi,$$

où V^{*U}_χ est l'espace des vecteurs $v \in V^{*U}$ pour lesquels D agit par χ. $V^{*U} \neq 0$ indique qu'il existe $\chi \in \widehat{D}$ tel que $V^{*U}_\chi \neq 0$. Ce qui montre que $\mathrm{Hom}_T(\tau_{|T}, \chi) \neq 0$ et donc que (π, V) n'est pas cuspidale. □

Proposition 4.5.3. *Le degré d'une représentation cuspidale est un multiple de $(q-1)$.*

Démonstration. $(\pi^*_{|U}, V^*)$ est une représentation de U. On regarde U comme un groupe abélien isomorphe à $\mathbb{F}_q$. Par la proposition 4.1.2 ψ est un caractère additif non-trivial de $\mathbb{F}_q$ et les caractères additifs non-triviaux de $\mathbb{F}_q$ sont donnés par

$x \mapsto \psi(ax),\ a \in \mathbb{F}_q$. On considère donc pour $a \in \mathbb{F}_q$ l'ensemble $V^*(a)$ des $\xi \in V^*$ tel que

$$\pi^* \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \xi = \psi(ax)\xi.$$

Comme (π, V) est cuspidale, par la proposition 4.5.2 $V^*(0)$ est nul. On peut donc écrire que $V^* = \bigoplus_{a \in \mathbb{F}_q^*} V^*(a)$. De plus si $a \in \mathbb{F}_q^*$ est fixé l'application $t \mapsto at$ est une bijection de $\mathbb{F}_q^*$ sur lui-même donc $V^* = \bigoplus_{t \in \mathbb{F}_q^*} V^*(at)$. Ensuite on remarque que pour pour tout $t \in \mathbb{F}_q^*$ l'application

$$\xi \mapsto \pi^* \begin{pmatrix} t^{-1} & 0 \\ 0 & 1 \end{pmatrix} \xi$$

est un isomorphisme entre $V^*(a)$ et $V^*(at)$.
On a donc $\dim(V) = \dim(V^*) = (q-1)\dim(V^*(a))$. Ce qui montre que le degré de (π, V) est un multiple de $q-1$. □

Et enfin :

Théorème 4.5.4. *Toute représentation cuspidale irréductible est de degré $q-1$.*

Démonstration. Pour démontrer ce résultat on utilise le fait que $\sum_{i=1}^h d_i^2 = |G|$ (propriété 2 p.9) où les d_i sont les degrés des représentations irréductibles de G. Après avoir enlevé de cette somme les termes correspondant aux représentations non cuspidales contruites précédemment il reste l'égalité suivante (où la somme s'effectue uniquement sur les représentations cuspidales) : $\sum_i d_i^2 = \frac{1}{2}(q^2-q)(q-1)^2$. Or on a vu qu'il y avait $\frac{1}{2}(q^2-q)$ représentations cuspidales irréductibles et que leur degré est un multiple de $q-1$. La seule solution est donc que le degré de toute représentation cuspidale irréductible soit exactement $q-1$. □

Remarque 4.5.5. On a aussi bien sûr que toute représentation cuspidale de degré $q-1$ est irréductible, ce qui est immédiat en remarquant que toute sous-représentation d'une représentation cuspidale est aussi cuspidale.

4.6 Construction des représentations cuspidales de $\mathrm{GL}_2(\mathbb{F}_q)$

Pour construire ces représentations nous allons d'abord, à l'aide du groupe d'Heisenberg et de la représentation de Weil construire un morphisme de $\mathrm{SL}_2(\mathbb{F}_q)$ dans $\mathrm{GL}(L^2(\mathbb{F}_{q^2}))$ où $L^2(G)$ est l'espace de Hilbert des fonctions de G dans $\mathbb{C}$ avec le produit scalaire hermitien suivant : $\langle f, g\rangle = \sum_{x \in G} f(x)\overline{g(x)}$. Ensuite nous construirons des sous-représentations de degré $q-1$ de cette dernière que nous étendrons à $\mathrm{GL}_2(\mathbb{F}_q)$. Pour finir nous verrons que les représentations ainsi construites sont bien cuspidales, irréductibles et au nombre de $\frac{1}{2}(q^2-q)$ à isomorphisme près.

4.6.1 Extension centrale, cocycle et représentations projectives

Dans cette partie nous allons un instant oublier le groupe $\mathrm{GL}_2(\mathbb{F}_q)$ et reprendre un groupe fini G quelconque dont on notera 1 le neutre. Nous utiliserons aussi $U(1)$ qui désigne les complexes de module 1. Voici d'abord quelques définitions importantes pour la suite.

Définition 4.6.1 (cocycle)**.** Un cocycle c est une fonction de $G \times G$ dans $U(1)$ qui vérifie :

$$\forall g, h, k \in G \quad c(g,h)c(gh,k) = c(g,hk)c(h,k).$$

On note $\mathrm{Z}^2(G, U(1))$ le groupe constitué par l'ensemble de ces cocycles (la loi étant la multiplication des fonctions induite par la multiplication dans $U(1)$).

Remarque 4.6.2. L'égalité qui caractérise un cocycle c implique que $\forall g \in G$ $c(g,1) = c(1,1)$ (prendre $h = k = 1$).

Définition 4.6.3 (cobord)**.** Un cobord c est une fonction de $G \times G$ dans $U(1)$ de la forme $c(g,h) = s(g)^{-1}s(h)^{-1}s(gh)$ où s est une fonction de G dans $U(1)$. On remarque alors que les cobords sont des cocycles et le sous-groupe de $\mathrm{Z}^2(G, U(1))$ constitué des cobords est noté $\mathrm{B}^2(G, U(1))$.

Définition 4.6.4 (Second groupe de cohomologie de G)**.** Le second groupe de cohomologie de G à coefficients dans $U(1)$ est le quotient $\mathrm{Z}^2(G, U(1))/\mathrm{B}^2(G, U(1))$, noté $\mathrm{H}^2(G, U(1))$.

Définition 4.6.5 (extension centrale de G par $U(1)$)**.** Une extension centrale de G par $U(1)$ est un groupe $\tilde{G}$ muni d'un morphisme α injectif de $U(1)$ dans $\tilde{G}$ et d'un morphisme β surjectif de $\tilde{G}$ dans G tels que $\ker(\beta) = \mathrm{Im}(\alpha)$.

Définition 4.6.6 (isomorphisme d'extensions centrales)**.** Soient $\tilde{G}$ muni de α et β et $\tilde{G}'$ muni de α' et β' deux extensions centrales de G. On dit que ces deux extensions centrales sont isomorphes si il existe un isomorphisme $\phi : \tilde{G} \to \tilde{G}'$ qui vérifie $\phi \circ \alpha = \alpha'$ et $\beta' \circ \phi = \beta$.

Il existe un lien important entre cocycles et extensions centrales :

Soit c un élément de $\mathrm{Z}^2(G, U(1))$. On définit alors le groupe $G(c) = G \times U(1)$ avec la multiplication suivante : $(g,z)(g',z') = (gg', zz'c(g,g')^{-1})$ et les applications α et β repectivement de $U(1)$ dans $G(c)$ et de $G(c)$ dans G définies par $\alpha(z) = (1, zc(1,1))$ et $\beta(g,z) = g$.

On a alors le résultat suivant :

Théorème 4.6.7. *$G(c)$ muni de α et β est une extension centrale de G par $U(1)$. Et si c' est un autre cocycle alors $G(c')$ muni de α' et β' définit une extension centrale de G par $U(1)$ isomorphe si et seulement si $c'c^{-1} \in \mathrm{B}^2(G, U(1))$.*

Démonstration. Le fait que $G(c)$ muni de α et β est bien une extension centrale de G par $U(1)$ est immédiat. Pour la suite supposons que $G(c)$ et $G(c')$ sont deux extensions isomorphes. On a alors un isomorphisme $\phi : G(c) \to G(c')$ tel que $\phi \circ \alpha = \alpha'$ et $\beta' \circ \phi = \beta$. Ceci implique donc que pour tout $g \in G$ il existe un unique $z(g) \in U(1)$ tel que $\phi(g,1) = (g, z(g))$. Alors, grâce à la remarque 4.6.2 et à l'égalité $\phi \circ \alpha = \alpha'$ on a que $\forall t \in U(1)$ et $\forall g, h \in G$

$\phi(g,t) = \phi((g,1) \cdot (1, tc(1,1))) = \phi(g,1) \cdot \phi(1, tc(1,1)) = (g, z(g)) \cdot (1, tc'(1,1))$
$= (g, z(g)t)$.

On utilise maintenant ceci pour calculer de deux façons $\phi((gh,1))$: d'une part

$\phi(gh,1) = \phi((g,1) \cdot (h, c(g,h))) = (g, z(g)) \cdot (h, z(h)c(g,h))$
$= (gh, z(g)z(h)c(g,h)c'(g,h)^{-1})$, d'autre part

$\phi((gh,1)) = (gh, z(gh))$.

Ainsi on obtient que $\forall g, h \in G$

$$c(g,h)c'(g,h)^{-1} = z(g)^{-1}z(h)^{-1}z(gh).$$

Ce qui veut dire que $c'c^{-1} \in \mathrm{B}^2(G, U(1))$.

Réciproquement on suppose que $c'c^{-1} \in \mathrm{B}^2(G, U(1))$. Cela signifie qu'il existe une application z de G dans $U(1)$ telle que $\forall g, h \in G$

$$c(g,h)c'(g,h)^{-1} = z(g)^{-1}z(h)^{-1}z(gh).$$

On définit alors $\phi : G(c) \to G(c')$ par $\phi(g,t) = (g, tz(g))$. On vérifie alors sans problème que c'est bien un isomorphisme et qu'il vérifie $\phi \circ \alpha = \alpha'$ et $\beta' \circ \phi = \beta$. $\square$

Voyons comment grâce à ce que l'on appelle une représentation projective de G on peut obtenir une représentation d'une extension centrale de G.

Définition 4.6.8 (représentation projective)**.** Soit $\mathcal{P}$ un espace de Hilbert et $U(\mathcal{P})$ l'ensemble des automorphismes unitaires de $\mathcal{P}$. Une représentation projective de G sur $\mathcal{P}$ est une fonction $\eta : G \to U(\mathcal{P})$ telle qu'il existe $c : G \times G \to U(1)$ avec $\eta(gh) = c(g,h)\eta(g)\eta(h)$.

On vérifie alors aisément que la fonction c associée à une représentation projective est un cocycle. La proposition suivante nous montre comment construire à partir d'une représentation projective une représentation d'une extension centrale de G :

Proposition 4.6.9. *Soit η une représentation projective de G sur $\mathcal{P}$ et c le cocycle associé. Alors $\tilde{\eta} : G(c) \to U(\mathcal{P})$ défini par $\tilde{\eta}(g,z) = z\eta(g)$ est une représentation de $G(c)$ sur $\mathcal{P}$.*

Démonstration. Soient $g, g' \in G$ et $z, z' \in U(1)$:
$\tilde{\eta}((g,z)(g',z')) = \tilde{\eta}(gg', zz'c(g,g')^{-1}) = zz'c(g,g')^{-1}\eta(gg') =$
$zz'c(g,g')^{-1}c(g,g')\eta(g)\eta(g') = z\eta(g)z'\eta(g') = \tilde{\eta}(g,z)\tilde{\eta}(g',z')$.
Ce qui prouve que $\tilde{\eta}$ est un morphisme de groupe. □

4.6.2 Le groupe d'Heisenberg et sa représentation de Heisenberg

Dans cette partie on prend G un groupe abélien fini, noté additivement (le neutre est donc noté 0). On va commencer par définir certains éléments particuliers de $U(L^2(G))$ pour construire une représentation projective de $G \times \widehat{G}$ sur $L^2(G)$:

Soient $x \in G$ et $\chi \in \widehat{G}$. On définit alors les opérateurs T_x et M_χ de $U(L^2(G))$ par : $\forall y \in G \ \ (T_x f)(y) = f(y-x)$ et $(M_\chi f)(y) = \chi(y)f(y)$.

Proposition 4.6.10. *L'application $\eta : G \times \widehat{G} \to U(L^2(G))$ définie par $\eta(x,\chi) = T_x M_\chi$ est une représentation projective de $G \times \widehat{G}$ sur $L^2(G)$.*

Démonstration. $\forall x, x' \in G$ et $\chi, \chi' \in \widehat{G}$:
$\eta((x,\chi)(x',\chi')) = \eta(x+x', \chi+\chi') = T_{x+x'}M_{\chi+\chi'} = T_x T_{x'} M_\chi M\chi' =$
$T_x(\chi(-x')M_\chi T_{x'})M_{\chi'} = \chi(-x')\eta(x,\chi)\eta(x',\chi')$. □

La démonstration montre donc aussi que le cocycle associé à cette représentation projective est $c((x,\chi),(x',\chi')) = \chi(x')^{-1}$. On a donc maintenant tous les éléments pour définir le groupe d'Heisenberg :

Définition 4.6.11 (Groupe d'Heisenberg)**.** Le groupe d'Heisenberg $H(G)$ d'un groupe fini abélien G est l'extension centrale de $G \times \widehat{G}$ par $U(1)$ associée au cocycle c défini ci-dessus.

Concrètement $H(G) = G \times \widehat{G} \times U(1)$ avec la multiplication suivante :

$$(x,\chi,z)(x',\chi',z') = (x+x', \chi+\chi', zz'\chi(x')).$$

De plus à partir de η et de la proposition 4.6.9 on obtient une représentation $\tilde{\eta}$ de $H(G)$ sur $L^2(G)$ définie par :

$$\tilde{\eta}(x',\chi',z')f(x) = z'\eta(x',\chi')f(x) = z'\chi'(x-x')f(x-x').$$

On va maintenant définir une représentation de $H(G)$ de façon induite, puis nous verrons qu'il s'agit de nouveau de $(\tilde{\eta}, L^2(G))$:

On pose $E = \{0\} \times \widehat{G} \times U(1)$ le sous groupe distingué de $H(G)$. Et on note $\theta : E \to \mathbb{C}^*$ le morphisme de groupe de E défini par $\theta(0,\chi,z) = z$. Ainsi on construit la représentation induite $\theta^{H(G)}$ de $H(G)$ sur l'espace suivant :

$$I = \{f : H(G) \to \mathbb{C} | f(eg) = \theta(e)f(g) \text{ pour tout } e \in E, g \in H(G)\}.$$

Si $f \in I$ on définit l'élément $\tilde{f} \in L^2(G)$ par $\tilde{f}(x) = f(-x,0,1)$. On a alors le résultat suivant :

Proposition 4.6.12. *Le morphisme $f \mapsto \tilde{f}$ est un isomophisme de I sur $L^2(G)$.*

Démonstration. Soit $g \in L^2(G)$. Si il existe $f \in I$ tel que $g = \tilde{f}$ on a alors que $\forall$ $(x,\chi,z) \in H(G)$,

$$f(x,\chi,z) = f((0,\chi,z\chi(x)^{-1})(x,0,1)) = \theta(0,\chi,z\chi(x)^{-1})f(x,0,1) = z\chi(x)^{-1}g(-x),$$

ce qui montre l'unicité de l'antécédent, puis pour l'existence il suffit de définir $f : H(G) \to \mathbb{C}$ par : $\forall$ $(x,\chi,z) \in H(G)$, $f(x,\chi,z) = z\chi(x)^{-1}g(-x)$, et de montrer que $f \in I$: Soit $(0,\chi,z) \in E$ et $(x',\chi',z') \in H(G)$,

$f((0,\chi,z)(x',\chi',z')) = f(x',\chi+\chi',zz'\chi(x')) = zz'\chi(x')((\chi+\chi')(x'))^{-1}g(-x') =$
$zz'\chi(x')\chi(x')^{-1}\chi'(x')^{-1}g(-x') = zz'\chi'(x')^{-1}g(-x') = \theta(0,\chi,z)fx',\chi',z')$,
ce qui montre bien que $f \in I$. □

De plus si $g' = (x',\chi',z') \in H(G)$ alors $\forall x \in G$,

$g' \cdot \tilde{f}(x) = g' \cdot f(-x,0,1) = f(x'-x,\chi',z') = f((0,\chi',z'\chi'(x-x')^{-1})(x'-x,0,1)) =$
$z'\chi'(x'-x)^{-1}f(x'-x,0,1) = z'\chi'(x-x')\tilde{f}(x-x')$,
ce qui montre que $(\theta^{H(G)}, I)$ et $(\tilde{\eta}, L^2(G))$ sont deux représentations isomorphes de $H(G)$.

Voyons maintenant un théorème très important, où $Z = \{0\} \times \{0\} \times U(1)$ est un sous-groupe de $H(G)$:

Théorème 4.6.13. *[PRA, Théorème 3.16] La représentation $\tilde{\eta}$ est irréductible. De plus toute représentation de $H(G)$ sur laquelle Z agit par l'identité de $U(1)$ est isomorphe à $\tilde{\eta}$.*

Remarque 4.6.14. Pour démontrer l'irréductibilité de $\tilde{\eta}$ on regarde $\tilde{\eta}$ comme $\theta^{H(G)}$ puis on utilise le corollaire 2.3.8.

Notons $B_0(G)$ l'ensemble des automorphismes de $H(G)$ agissant par l'identité sur Z. Si $\sigma \in B_0(G)$ on vérifie rapidement que ${}^\sigma\tilde{\eta}$ définie par ${}^\sigma\tilde{\eta}(g) = \tilde{\eta}(\sigma^{-1}(g))$ est une représentation de $H(G)$ pour laquelle Z agit par l'identité de $U(1)$. Par le théorème précédent on a donc que ${}^\sigma\tilde{\eta}$ et $\tilde{\eta}$ sont isomorphes donc il existe $\nu(\sigma)$: $L^2(G) \to L^2(G)$ telle que $\forall g \in H(G)\ \ \nu(\sigma) \circ \tilde{\eta}(g) = {}^\sigma\tilde{\eta}(g) \circ \nu(\sigma)$. De plus un calcul rapide montre que $\nu(\sigma) \circ \nu(\sigma') \circ \tilde{\eta}(g) = {}^{\sigma\sigma'}\tilde{\eta}(g) \circ \nu(\sigma) \circ \nu(\sigma')$ donc par la proposition 2.1.7 on obtient que $\sigma \mapsto \rho(\sigma) := \nu(\sigma^{-1})$ est une représentation projective de $B_0(G)$ sur $L^2(G)$. Cette représentation est appelée représentation de Weil.

Il s'agit maintenant d'obtenir une expression de $\nu(\sigma)$. Dans ce but il est plus simple de penser à $(\tilde{\eta}, L^2(G))$ comme $(\theta^{H(G)}, I)$. I est un sous-espace de $\mathbb{C}[H(G)]$, et on note r la représentation de $H(G)$ sur $\mathbb{C}[H(G)]$ où $H(G)$ agit comme suit

$$r(g')f(g) = f(gg').$$

On voit alors facilement que $\nu_r(\sigma) : \mathbb{C}[H(G)] \to \mathbb{C}[H(G)]$ défini par $(\nu_r(\sigma)f)(g) = f({}^\sigma g)$ est un isomorphisme entre les représentations r et ${}^\sigma r$. Malheureusement si $f \in I$, $\nu_r(\sigma)f$ ne l'est pas forcément. En revanche en modifiant un peu l'expression de $\nu_r(\sigma)$ comme suit :

$$(\nu'_r(\sigma)f)(g) = \frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, \chi, 1)g)),$$

on obtient alors cette fois que I est invariant par $\nu'_r(\sigma)$ par le calcul suivant :

$(\nu'_r(\sigma)f)((0, \chi', z')(x'', \chi'', z'')) = \frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, \chi, 1)(0, \chi', z')(x'', \chi'', z''))) =$
$\frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, \chi + \chi', z')(x'', \chi'', z''))) =$
$\frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, 0, z')(0, \chi + \chi', 1)(x'', \chi'', z''))) =$
$\frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} z' f({}^\sigma((0, \chi + \chi', 1)(x'', \chi'', z'')))$ (car Z invariant par σ et $f \in I$)
$= z' \frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, \chi, 1)(x'', \chi'', z'')))$ (car $\chi \mapsto \chi + \chi'$ est une bijection de $\widehat{G}$)
$= \theta(0, \chi', z')(\nu'_r(\sigma)f)(x'', \chi'', z'')$.

De plus $\nu'_r(\sigma)$ est un automorphisme de I, c'est donc un isomorphisme entre les représentations $(\theta^{H(G)}, I)$ et $({}^\sigma\theta^{H(G)}, I)$, on vient donc de construire $\nu(\sigma)$:

$$\forall f \in H(G),\ g \in G\ \ (\nu(\sigma)f)(g) = \frac{1}{|\widehat{G}|} \sum_{\chi \in \widehat{G}} f({}^\sigma((0, \chi, 1)g)).$$

La question qui se pose alors est de savoir quels sont concrètement les éléments de $B_0(G)$. On rappelle que $H(G)$ a été construit à partir du cocycle défini par $c((x, \chi), (x', \chi')) = \chi(x')^{-1}$ et on définit alors $Q : G \times \widehat{G} \to U(1)$ par

$Q((x,\chi),(x',\chi')) = \chi(x')$. Avec cette notation la multiplication sur $H(G)$ s'écrit

$$(x,\chi,z)(x',\chi',z') = (x+x',\chi+\chi',zz'Q((x,\chi),(x',\chi'))).$$

Le théorème suivant nous donne alors un moyen de construire des éléments de $B_0(G)$.

Proposition 4.6.15. *Soit* $Q : G \times \widehat{G} \to U(1)$ *tel que* $\forall\ (x,\chi,z),(x',\chi',z') \in H(G)$,$(x,\chi,z)(x',\chi',z') = (x+x',\chi+\chi',zz'Q((x,\chi),(x',\chi')))$ *et* $\sigma \in \mathrm{Aut}(G\times\widehat{G})$ *tel que* $\forall x,x' \in G,\ \forall \chi,\chi' \in \widehat{G}\ Q(\sigma(x,\chi),\sigma(x',\chi')) = Q((x,\chi),(x',\chi'))$*, alors* $\tilde{\sigma} : H(G) \to H(G)$ *défini par* $\tilde{\sigma}(x,\chi,z) = (\sigma(x,\chi),z)$ *est un élément de* $B_0(G)$*.*

Démonstration. Le caractère bijectif de $\tilde{\sigma}$ est évident puisque σ réalise une bijection de $G\times\widehat{G}$. Il reste donc à montrer que c'est un morphisme. Soit $(x,\chi),(x',\chi') \in G\times\widehat{G}$:

$$\begin{aligned}
&\tilde{\sigma}((x,\chi,z)(x',\chi',z')) = \tilde{\sigma}(x+x',\chi+\chi',zz'Q((x,\chi),(x',\chi'))) = \\
&(\sigma(x+x',\chi+\chi'),zz'Q((x,\chi),(x',\chi'))) = \\
&(\sigma((x,\chi)+(x',\chi')),zz'Q(\sigma(x,\chi),\sigma(x',\chi'))) = \\
&(\sigma(x,\chi)+\sigma(x',\chi'),zz'Q(\sigma(x,\chi),\sigma(x',\chi'))) = \\
&(\sigma(x,\chi),z)(\sigma(x',\chi'),z') = \tilde{\sigma}(x,\chi,z)\tilde{\sigma}(x',\chi',z').
\end{aligned}$$

$\square$

Cela donne donc un moyen de construire des éléments de $B_0(G)$ à partir de ceux de $\mathrm{Aut}(G\times\widehat{G})$ sous certaines conditions.

Si $x \mapsto 2x$ est un automorphisme de G alors $\phi : H(G) \to H(G)$ défini par $\phi(x,\chi,z) = (x,\chi,z\chi(-\frac{x}{2}))$ est une bijection de $H(G)$ dans lui-même ($(x,\chi,z) \mapsto (x,\chi,z\chi(\frac{x}{2}))$ donnant la réciproque). Ceci permet de définir une nouvelle multiplication m' dans $H(G)$ telle que $\phi((x,\chi,z)(x',\chi',z')) = m'(\phi(x,\chi,z),\phi(x',\chi',z'))$. Le calcul donne

$$m'((x,\chi,z),(x',\chi',z')) = (x+x',\chi+\chi',zz'\chi(\frac{x'}{2})\chi'(\frac{-x}{2})).$$

$\phi : (H(G),m) \to (H(G),m')$ devient alors un isomorphisme de groupes (où m est la multiplication de départ).

4.6.3 Application à la construction d'une représentation de $\mathrm{SL}_2(\mathbb{F}_q)$ sur $L^2(\mathbb{F}_{q^2})$

Dans cette partie nous allons appliquer ce qui précède au cas où G est le groupe additif $\mathbb{F}_{q^2}$ et en utilisant l'isomorphisme $x \mapsto (y \mapsto \psi(\mathrm{tr}(\bar{x}y)))$ de $\mathbb{F}_{q^2}$ dans $\widehat{\mathbb{F}_{q^2}}$

(proposition 4.1.3) on peut alors voir $H(\mathbb{F}_{q^2})$ comme $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times U(1)$ avec la multiplication m' définie plus haut qui donne ici :

$$m'((x,y,z),(x',y',z')) = (x+x', y+y', zz'\psi(\mathrm{tr}(\frac{1}{2}(\overline{y}x' - \overline{y'}x)))).$$

En posant $Q((x,y),(x',y')) = \psi(\mathrm{tr}(\frac{1}{2}(\overline{y}x' - \overline{y'}x)))$ on a,

$$m'((x,y,z),(x',y',z')) = (x+x', y+y', zz'Q((x,y),(x',y'))).$$

Puisque $\mathbb{F}_{q^2}$ et $\widehat{\mathbb{F}_{q^2}}$ sont isomorphes (en utilisant l'isomorphisme ci-dessus) et que $\mathbb{F}_{q^2}$ est un $\mathbb{F}_q$-espace vectoriel de dimension 2 on peut donc voir $\mathrm{GL}_2(\mathbb{F}_q)$ comme un sous-groupe de $\mathrm{Aut}(\mathbb{F}_{q^2}, \widehat{\mathbb{F}_{q^2}})$. De plus si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$ le calcul montre que $Q(\sigma(x,y),\sigma(x',y')) = Q((ax+by, cx+dy),(ax'+by', cx'+dy')) = Q((x,y),(x',y'))$ donc par la proposition 4.6.15 $(x,y,z) \mapsto (ax+by, cx+dy, z)$ définit un élément de $B_0(\mathbb{F}_{q^2})$. Puis en ramenant cet automorphisme dans $H(\mathbb{F}_{q^2})$ avec la multiplication initiale par l'application ϕ^{-1} définie dans la partie précédente, on associe alors à σ l'élément de $B_0(\mathbb{F}_{q^2})$ (que l'on notera abusivement σ) défini par

$$(x,y,z) \mapsto (ax+by, cb+dy, z\psi(\frac{1}{2}\mathrm{tr}(-\overline{y}x + \overline{(cb+dy)}(ax+y)))).$$

$\mathrm{SL}_2(\mathbb{F}_q)$ peut alors être vu comme un sous-groupe de $B_0(\mathbb{F}_{q^2})$ et la représentation de Weil nous donne une représentation projective

$$\rho : \mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{GL}(L^2(\mathbb{F}_{q^2})).$$

Après de nombreux calculs ([PRA, p.24]) on trouve l'expression suivante de cette représentation projective : $\forall f \in L^2(\mathbb{F}_{q^2}),\ \forall x \in \mathbb{F}_{q^2}$

$$(\rho(\sigma)f)(x) = \begin{cases} \psi(dcN(x))f(x) & \text{si } b = 0 \\ \frac{1}{q^2}\sum_{y\in\mathbb{F}_{q^2}} \psi(\frac{dN(x) - \mathrm{tr}(\overline{y}x) + aN(y)}{b})f(y) & \text{sinon.} \end{cases}$$

Mais ceci n'est qu'une représentation projective. On définit alors $\tilde{\rho}$ de $\mathrm{SL}_2(\mathbb{F}_q)$ dans $\mathrm{GL}(L^2(\mathbb{F}_{q^2}))$ par : $\forall f \in L^2(\mathbb{F}_{q^2}),\ \forall x \in \mathbb{F}_{q^2}$

$$(\tilde{\rho}(\sigma)f)(x) = \begin{cases} \psi(dcN(x))f(x) & \text{si } b = 0 \\ \frac{-1}{q}\sum_{y\in\mathbb{F}_{q^2}} \psi(\frac{dN(x) - \mathrm{tr}(\overline{y}x) + aN(y)}{b})f(y) & \text{sinon.} \end{cases}$$

Et on a la proposition suivante :

Proposition 4.6.16. *[PRA, Proposition 3.26] La fonction $\tilde{\rho}$ de* $\mathrm{SL}_2(\mathbb{F}_q)$ *dans* $\mathrm{GL}(L^2(\mathbb{F}_{q^2}))$ *est une représentation de* $\mathrm{SL}_2(\mathbb{F}_q)$ *sur* $L^2(\mathbb{F}_{q^2})$.

Remarque 4.6.17. On sait déjà pour σ et σ' fixés qu'il existe $\lambda \in \mathbb{C}^*$ tel que $\tilde{\rho}(\sigma\sigma') = \lambda\tilde{\rho}(\sigma)\tilde{\rho}(\sigma')$. La démonstration de ce théorème consiste donc simplement à montrer que, pour f et x respectivement choisis dans $L^2(\mathbb{F}_{q^2})$ et $\mathbb{F}_{q^2}$ tels que $(\tilde{\rho}(\sigma\sigma')f)(x) \neq 0$, on a $(\tilde{\rho}(\sigma\sigma')f)(x) = (\tilde{\rho}(\sigma)\tilde{\rho}(\sigma')f)(x)$.

Comme annoncé nous avons bien construit explicitement une représentation de $\mathrm{SL}_2(\mathbb{F}_q)$ sur $L^2(\mathbb{F}_{q^2})$. Il reste donc, dans les parties suivantes, à trouver des sous-représentations cuspidales de degré $q-1$ de cette dernière et de les étendre à $\mathrm{GL}_2(\mathbb{F}_q)$.

4.6.4 Sous-représentations de degré $q-1$

Ici nous allons construire un sous-espace $\mathrm{SL}_2(\mathbb{F}_q)$-invariant pour la représentation $(\tilde{\rho}, L^2(\mathbb{F}_{q^2}))$ et de dimension $q-1$. On note $(\mathbb{F}_{q^2}^*)_x = \{y \in \mathbb{F}_{q^2}^* | N(y) = x\}$. Prenons ω un morphisme de groupe de $\mathbb{F}_{q^2}$ dans $\mathbb{C}^*$. Pour la suite il est important que la restriction de ω à $(\mathbb{F}_{q^2}^*)_1$ soit non-triviale. On utilise alors la proposition suivante :

Définition 4.6.18 (caractère primitif)**.** Soit ω un un morphisme de groupe de $\mathbb{F}_{q^2}$ dans $\mathbb{C}^*$. ω est dit primitif si $\forall \chi \in \widehat{\mathbb{F}_q^*} \;\; \omega \neq \chi \circ N$, où N désigne la norme sur $\mathbb{F}_{q^2}$.

Proposition 4.6.19. *Un morphisme de groupe de* $\mathbb{F}_{q^2}$ *dans* $\mathbb{C}^*$ *est primitif si et seulement si sa restriction à* $(\mathbb{F}_{q^2}^*)_1$ *est non-triviale.*

Démonstration. Soit ω ce morphisme de groupe de $\mathbb{F}_{q^2}$ dans $\mathbb{C}^*$. Si ω n'est pas primitif alors il est immédiat que sa restriction à $(\mathbb{F}_{q^2}^*)_1$ est triviale. Supposons maintenant que la restriction de ω à $(\mathbb{F}_{q^2}^*)_1$ est triviale, il s'agit de montrer que ω n'est pas primitif. Pour cela on va utiliser la propriété 6 de la partie 4.1 qui dit que pour $x \in \mathbb{F}_q^*$, le nombre d'éléments $y \in \mathbb{F}_{q^2}^*$ tels que $N(y) = x$ est $q+1$. On note alors z_x un élément de $(\mathbb{F}_{q^2}^*)_x$. On remarque que $\forall x, x' \in \mathbb{F}_q \;\; (\mathbb{F}_{q^2}^*)_{xx'} = z_x(\mathbb{F}_{q^2}^*)_{x'}$ (en utilisant une inclusion puis le cardinal) donc par hypothèse on a $\forall y \in (\mathbb{F}_{q^2}^*)_x \;\; \omega(y) = \omega(z_x)$. Pour $x \in \mathbb{F}_q^*$ on pose $\chi(x) = \omega(z_x)$, qui ne dépend pas du choix de z_x d'après ce qui précède. $\forall x, x' \in \mathbb{F}_q \; \exists y_{x'} \in (\mathbb{F}_{q^2}^*)_{x'}$ tel que $z_{xx'} = z_x y_{x'}$ donc $\chi(xx') = \omega(z_{xx'}) = \omega(z_x y_{x'}) = \omega(z_x)\omega(y_{x'}) = \omega(z_x)\omega(z_{x'}) = \chi(x)\chi(x')$. Ce qui montre que $\chi \in \widehat{\mathbb{F}_q^*}$, de plus si $y \in \mathbb{F}_{q^2}^* \;\; \omega(y) = \omega(z_{N(y)}) = \chi(N(y))$ donc $\omega = \chi \circ N$ n'est pas primitif. $\square$

On choisit donc ω un morphisme de groupe de $\mathbb{F}_{q^2}$ dans $\mathbb{C}^*$ primitif, et on considère le sous-espace W_ω suivant :

$$W_\omega = \{f \in L^2(\mathbb{F}_{q^2}) | f(yx) = \omega(y)^{-1} f(x) \;\; \forall y \in (\mathbb{F}_{q^2}^*)_1\}.$$

Montrons que W_ω est $\mathrm{SL}_2(\mathbb{F}_q)$-invariant pour $(\tilde{\rho}, L^2(\mathbb{F}_{q^2}))$.

Tout d'abord on peut se restreindre à montrer l'invariance de W_ω pour les matrices $t(a)$,$u(c)$ et ω qui engendrent $\mathrm{SL}_2(\mathbb{F}_q)$ par la proposition 4.2.3.

Ensuite grâce aux formules explicites de $\tilde{\rho}$ on montre que $\forall f \in L^2(\mathbb{F}_{q^2})$ et $\forall x \in \mathbb{F}_{q^2}$

$$(\tilde{\rho}(t(a))f)(x) = f(a^{-1}x),$$
$$(\tilde{\rho}(u(c))f)(x) = \psi(cN(x))f(x),$$
$$(\tilde{\rho}(\omega)f)(x) = \frac{-1}{q}\sum_{y\in\mathbb{F}_{q^2}} \overline{x(y)}f(y),$$

où $x(y) = \psi(\mathrm{tr}(\bar{x}y))$.

Ce qui permet de montrer la stabilité de W_ω par $\tilde{\rho}(\sigma)$ $\forall\sigma \in \mathrm{SL}_2(\mathbb{F}_q)$.

Et voici le dernier résultat important de cette partie.

Proposition 4.6.20. *Si ω est primitif alors W_ω est de dimension $q-1$.*

Démonstration. Tout d'abord puisque ω est primitif il existe $y \in (\mathbb{F}_{q^2}^*)_1$ tel que $\omega(y) \neq 1$. Ainsi $f(0) = f(0y) = \omega(y)^{-1}f(0)$ montre que $\forall f \in W_\omega$ $f(0) = 0$. Ensuite on utilise les notations et résultats de la démonstration de la propositon 4.6.19. Pour $x \in \mathbb{F}_q^*$ $(\mathbb{F}_{q^2}^*)_x = z_x(\mathbb{F}_{q^2}^*)_1$ donc l'image par f d'un élément de norme x est complètement déterminée par celle de z_x. La donnée de $f(z_x)$ pour tout $x \in \mathbb{F}_q^*$ détermine donc entièrement f. Réciproquement se donner $f \in W_\omega$ revient à donner l'image par f d'un élément de chaque $(\mathbb{F}_{q^2}^*)_x$ pour $x \in \mathbb{F}_q^*$. Or $|\mathbb{F}_q^*| = q-1$ donc $\dim(W_\omega) = q-1$. $\square$

On obtient donc une représentation $(\tilde{\rho}_\omega, W_\omega)$ de $SL_2(\mathbb{F}_q)$ de degré $q-1$.

4.6.5 Extension à $\mathrm{GL}_2(\mathbb{F}_q)$

Dans cette partie on va étendre $(\tilde{\rho}_\omega, W_\omega)$ en une représentation de degré $q-1$ de $\mathrm{GL}_2(\mathbb{F}_q)$.

On remarque tout d'abord que si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ alors

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & \det(\sigma) \end{pmatrix} \begin{pmatrix} a & b \\ \frac{c}{\det(\sigma)} & \frac{d}{\det(\sigma)} \end{pmatrix}.$$

Or $\begin{pmatrix} a & b \\ \frac{c}{\det(\sigma)} & \frac{d}{\det(\sigma)} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$ donc toute matrice de $\mathrm{GL}_2(\mathbb{F}_q)$ est, de façon unique, le produit d'une matrice de la forme $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ et d'une matrice de $\mathrm{SL}_2(\mathbb{F}_q)$.

$\forall a \in \mathbb{F}_q^*$ on commence par définir

$$\left(\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix} f\right)(x) = \omega(\tilde{a})f(\tilde{a}x),$$

où $\tilde{a} \in (\mathbb{F}_{q^2}^*)_a$. Et on peut rapidement vérifier que la définition précédente ne dépend pas du choix de $\tilde{a}$ dans $(\mathbb{F}_{q^2}^*)_a$.

Ensuite on étend donc naturellement $(\tilde{\rho}_\omega, W_\omega)$ à $\mathrm{GL}_2(\mathbb{F}_q)$ de la façon suivante :

Pour $\sigma \in \mathrm{SL}_2(\mathbb{F}_q)$

$$\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\right) = \tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\tilde{\rho}(\sigma).$$

Pour finir il faut vérifier que l'on a toujours bien un morphisme, c'est-à-dire que $\forall a, a' \in \mathbb{F}_q^*$ et $\forall \sigma, \sigma' \in \mathrm{SL}_2(\mathbb{F}_q)$,

$$\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\sigma'\right) = \tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\right)\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\sigma'\right).$$

On commence donc par montrer que pour tout $\sigma \in \mathrm{SL}_2(\mathbb{F}_q)$ on a

$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}^{-1} = \tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}^{-1}\right).$$

Pour cela on le montre d'abord pour les matrices $t(a)$, $u(c)$ et ω puis on étend le résultat à $\sigma \in \mathrm{SL}_2(\mathbb{F}_q)$ en utilisant la proposition 4.2.3.

Ensuite on remarque aisément à partir de la définition que

$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix} = \tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}.$$

Puis on conclut par le calcul suivant :

$$\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\sigma'\right) = \tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\left[\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}\sigma\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\sigma'\right]\right) =$$

$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}\sigma\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}^{-1}\right)\tilde{\rho}(\sigma') =$$

$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}^{-1}\tilde{\rho}(\sigma') =$$

$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}^{-1}\tilde{\rho}(\sigma)\tilde{\rho}(\sigma') =$$
$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'^{-1}\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}(\sigma') = \tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & aa'\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}(\sigma') =$$
$$\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}(\sigma') = \tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\tilde{\rho}(\sigma)\tilde{\rho}\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\tilde{\rho}(\sigma') =$$
$$\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\sigma\right)\tilde{\rho}\left(\begin{pmatrix}1 & 0\\ 0 & a'\end{pmatrix}\sigma'\right).$$

On obtient donc bien une représentation $(\tilde{\rho}_\omega, W_\omega)$ de $\mathrm{GL}_2(\mathbb{F}_q)$ de degré $q-1$.

4.6.6 Représentations cuspidales de $\mathrm{GL}_2(\mathbb{F}_q)$

Dans cette partie nous allons montrer que, grâce aux représentations $(\tilde{\rho}_\omega, W_\omega)$, nous avons construit toutes les représentations cuspidales irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$.

Proposition 4.6.21. *Pour tout caractère primitif ω de $\mathbb{F}_{q^2}^*$ la représentation $(\tilde{\rho}_\omega, W_\omega)$ est cuspidale.*

Démonstration. On va montrer que W_ω ne contient pas de vecteur non nul fixe par l'action de U. On note $\overline{U}$ le sous-groupe des matrices de la forme $\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$, $c \in \mathbb{F}_q$. On constate alors que $\omega\overline{U}\omega^{-1} = U$ donc f est fixe par U si et seulement si $\tilde{\rho}_\omega(\omega)f$ est fixe par $\overline{U}$. Il suffit donc de montrer que W_ω ne contient pas de vecteur non nul fixe par l'action de $\overline{U}$. Soit $f \in W_\omega$ que l'on suppose invariant par l'action de $\overline{U}$. Tout d'abord on a vu dans la démonstration de la proposition 4.6.20 que $f(0) = 0$. Ensuite si $x \in \mathbb{F}_q^*$ on a $\forall c \in \mathbb{F}_q$

$$f(x) = \left(\tilde{\rho}_\omega\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}f\right)(x) = \psi(cN(x))f(x).$$

Puisque ψ non-trivial et $x \in \mathbb{F}_q^*$ on peut choisir $c \in \mathbb{F}_q$ tel que $\psi(cN(x)) \neq 1$. Ainsi l'égalité ci-dessus montre que $\forall x \in \mathbb{F}_q$ $f(x) = 0$, donc $f = 0$. □

$(\tilde{\rho}_\omega, W_\omega)$ est donc une représentation cuspidale de degré $q-1$ de $\mathrm{GL}_2(\mathbb{F}_q)$, elle est donc irréductible d'après la remarque 4.5.5. Il reste donc à savoir si ces représentations sont isomorphes deux à deux.

Proposition 4.6.22. *Soient ω_1 et ω_2 deux caractères primitifs de $\mathbb{F}_{q^2}^*$. Si les représentations cuspidales $(\tilde{\rho}_{\omega_1}, W_{\omega_1})$ et $(\tilde{\rho}_{\omega_2}, W_{\omega_2})$ sont isomorphes alors $\omega_1 = \omega_2$ ou $\omega_2 = \omega_1 \circ F$ (où F est l'automorphisme de Frobenius).*

Démonstration. On montre ce résultat par contraposée. On suppose donc que $\omega_1 \neq \omega_2$ et $\omega_2 \neq \omega_1 \circ F$. On note respectivement χ_1 et χ_2 les caractères associés à $(\tilde{\rho}_{\omega_1}, W_{\omega_1})$ et $(\tilde{\rho}_{\omega_2}, W_{\omega_2})$. Pour $u \in \mathbb{F}_q^*$ on fixe $\tilde{u} \in \mathbb{F}_{q^2}$ tel que $N(\tilde{u}) = u$. Ensuite on note 1_u l'élément de W_{ω_1} tel que $1_u(\tilde{u}) = 1$ et $1_u(x) = 0$ si $N(x) \neq u$. L'ensemble $\{1_u | u \in \mathbb{F}_q^*\}$ est une base de W_{ω_1} (voir la démonstration de la proposition 4.6.20). Ainsi pour tout $\sigma \in \mathrm{GL}_2(\mathbb{F}_q)$,

$$\chi_1(\sigma) = \mathrm{tr}(\tilde{\rho}_{\omega_1}(\sigma)) = \sum_{u \in \mathbb{F}_q^*} (\tilde{\rho}_{\omega_1}(\sigma) 1_u)(\tilde{u}).$$

En utilisant les formules donnant $\tilde{\rho}_{\omega_1}(\sigma)$ pour $\sigma \in \mathrm{SL}_2(\mathbb{F}_q)$ et l'extension à $\mathrm{GL}_2(\mathbb{F}_q)$ vue précédemment on peut donc calculer les valeurs de χ_1 : Si $\sigma = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$:

$$(\tilde{\rho}_{\omega_1}(\sigma) 1_u)(\tilde{u}) = \left(\tilde{\rho}_{\omega_1} \left(\begin{pmatrix} 1 & 0 \\ 0 & a^2 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right) 1_u \right)(\tilde{u}) = \omega_1(a) 1_u(a^{-1} a \tilde{u}) = \omega_1(a).$$

On a utilisé ici le fait que $N(a) = a^2$ car $a \in \mathbb{F}_q^*$. Ainsi $\mathrm{tr}\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right) = \sum_{u \in \mathbb{F}_q^*} \omega_1(a) = (q-1)\omega_1(a)$.

Pour les autres classes de conjugaisons le calcul donne :

$$\mathrm{tr}\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \right) = -\omega_1(a).$$

$$\mathrm{tr}\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right) = 0.$$

Pour finir les éléments de $\mathrm{GL}_2(\mathbb{F}_q)$ dont le polynôme caractéristique est irréductible sur $\mathbb{F}_q$ sont semblables à des éléments de la forme $\begin{pmatrix} 0 & -a \\ 1 & b \end{pmatrix}$ avec $X^2 - bX + a$ irréductible dans $\mathbb{F}_q$ mais ayant donc deux racines conjuguées s et $F(s)$ dans $\mathbb{F}_{q^2}$. On a alors le résultat suivant :

$$\mathrm{tr}\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} \right) = -\omega_1(s) - \omega_1(F(s)).$$

Démonstration. On commence par calculer $\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} 0 & -a \\ 1 & b \end{pmatrix} 1_u \right)(\tilde{u})$.

$$\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} 0 & -a \\ 1 & b \end{pmatrix} \tilde{f} \right)(x) = \left(\tilde{\rho}_{\omega_1} \left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & -a \\ a^{-1} & a^{-1}b \end{pmatrix} \right) \tilde{f} \right)(x) =$$
$$\left(\tilde{\rho}_{\omega_1} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \tilde{\rho}_{\omega_1} \begin{pmatrix} 0 & -a \\ a^{-1} & a^{-1}b \end{pmatrix} \tilde{f} \right)(x) =$$

$\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\left(x \mapsto \frac{-1}{q}\sum_{y\in\mathbb{F}_{q^2}}\psi(\frac{a^{-1}bN(x)-\mathrm{tr}(\overline{y}x)}{-a})\tilde{f}(y)\right)\right)(x) =$
$\frac{-\omega_1(\tilde{a})}{q}\sum_{y\in\mathbb{F}_{q^2}}\psi(\frac{a^{-1}bN(\tilde{a}x)-\mathrm{tr}(\overline{y}\tilde{a}x)}{-a})\tilde{f}(y)$ avec $\tilde{a}$ tel que $N(\tilde{a}) = a$
$= \frac{-\omega_1(\tilde{a})}{q}\sum_{y\in\mathbb{F}_{q^2}}\psi(\frac{\mathrm{tr}(\overline{y}\tilde{a}x)-bN(x)}{a})\tilde{f}(y)$
Donc :
$\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & -a\\ 1 & b\end{pmatrix}1_u\right)(\tilde{u}) = \frac{-\omega_1(\tilde{a})}{q}\sum_{y\in\mathbb{F}_{q^2}}\psi(\frac{\mathrm{tr}(\overline{y}\tilde{a}\tilde{u})-bN(\tilde{u})}{a})1_u(y)$

Or $1_u(y) \neq 0$ si et seulement si $y \in (\mathbb{F}_{q^2}^*)_u = \tilde{u}(\mathbb{F}_{q^2}^*)_1$, et dans ce cas $1_u(y) = 1_u(z\tilde{u}) = \omega_1(z)^{-1}$ avec $z \in (\mathbb{F}_{q^2}^*)_1$, donc :
$\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & -a\\ 1 & b\end{pmatrix}1_u\right)(\tilde{u}) = \frac{-\omega_1(\tilde{a})}{q}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\psi(\frac{\mathrm{tr}(\overline{z\tilde{u}}\tilde{a}\tilde{u})-bN(\tilde{u})}{a})\omega_1(z)^{-1}$
$= \frac{-\omega_1(\tilde{a})}{q}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\psi(\frac{\mathrm{tr}(\overline{z}\tilde{a}u)-bu}{a})\omega_1(z)^{-1}$ car $N(\tilde{u}) = \tilde{u}\overline{\tilde{u}} = u$
$= \frac{-\omega_1(\tilde{a})}{q}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\psi(\frac{z^{-1}\tilde{a}u+z\overline{\tilde{a}u}-bu}{a})\omega_1(z)^{-1}$ car $\overline{z} = z^{-1}$ et $\mathrm{tr}(x) = x + \overline{x}$
$= \frac{-\omega_1(\tilde{a})}{q}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\psi(\frac{u(z^{-1}\tilde{a}+z\overline{\tilde{a}}-b)}{a})\omega_1(z)^{-1}$ car $\overline{u} = u$

On peut donc maintenant calculer $\mathrm{tr}\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & a\\ 1 & b\end{pmatrix}\right)$:

$\mathrm{tr}\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & a\\ 1 & b\end{pmatrix}\right) = \frac{-\omega_1(\tilde{a})}{q}\sum_{u\in(\mathbb{F}_q^*)}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\psi(\frac{u(z^{-1}\tilde{a}+z\overline{\tilde{a}}-b)}{a})\omega_1(z)^{-1}$
$= \frac{-\omega_1(\tilde{a})}{q}\sum_{z\in(\mathbb{F}_{q^2}^*)_1}\omega_1(z)^{-1}\sum_{u\in(\mathbb{F}_q^*)}\psi(\frac{u(z^{-1}\tilde{a}+z\overline{\tilde{a}}-b)}{a})$.

$z^{-1}\tilde{a} + z\overline{\tilde{a}} - b = 0 \Leftrightarrow \overline{\tilde{a}}\tilde{a} + (z\overline{\tilde{a}})^2 - b(z\overline{\tilde{a}}) = 0$
$\Leftrightarrow (z\overline{\tilde{a}})^2 - b(z\overline{\tilde{a}}) + a = 0 \Leftrightarrow (z\overline{\tilde{a}} = s$ ou $z\overline{\tilde{a}} = F(s))$
$\Leftrightarrow (z = \tilde{a}a^{-1}s$ ou $z = \tilde{a}a^{-1}F(s))$
On vérifie rapidement que $\tilde{a}a^{-1}s$ et $\tilde{a}a^{-1}F(s))$ sont bien dans $(\mathbb{F}_{q^2}^*)_1$. Ensuite :
Si $z = \tilde{a}a^{-1}s$ ou $z = \tilde{a}a^{-1}F(s)$:

$$\sum_{u\in(\mathbb{F}_q^*)}\psi(\frac{u(z^{-1}\tilde{a}+z\overline{\tilde{a}}-b)}{a}) = q-1$$

Et si $z \neq \tilde{a}a^{-1}s$ et $z \neq \tilde{a}a^{-1}F(s)$:

$$\sum_{u\in(\mathbb{F}_q^*)}\psi(\frac{u(z^{-1}\tilde{a}+z\overline{\tilde{a}}-b)}{a}) = \sum_{u\in(\mathbb{F}_q^*)}\psi(u) = -1$$

Ainsi on obtient :

$\mathrm{tr}\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & a\\ 1 & b\end{pmatrix}\right) = \frac{-\omega_1(\tilde{a})}{q}(\sum_{z\in(\mathbb{F}^*_{q^2})_1}(-\omega_1(z)^{-1})+\omega_1(\tilde{a}a^{-1}s)^{-1}+\omega_1(\tilde{a}a^{-1}F(s))^{-1}$
$+(q-1)\omega_1(\tilde{a}a^{-1}s)^{-1}+(q-1)\omega_1(\tilde{a}a^{-1}F(s))^{-1})$
$= \frac{-\omega_1(\tilde{a})}{q}(\sum_{z\in(\mathbb{F}^*_{q^2})_1}(-\omega_1(z)^{-1})+q(\omega_1(\tilde{a}a^{-1}s)^{-1})+q(\omega_1(\tilde{a}a^{-1}F(s))^{-1}))$
$= \frac{\omega_1(\tilde{a})}{q}(\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)^{-1})-\omega_1(as^{-1})-\omega_1(aF(s)^{-1})$
Or $sF(s)=a$ donc :
$\mathrm{tr}\left(\tilde{\rho}_{\omega_1}\begin{pmatrix}0 & a\\ 1 & b\end{pmatrix}\right) = \frac{\omega_1(\tilde{a})}{q}(\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)^{-1})-\omega_1(s)-\omega_1(F(s))$
Il reste donc maintenant à montrer que $A=\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)^{-1}=0$.

Tout d'abord puisque $z\mapsto z^{-1}$ est une bijection de $\mathbb{F}^*_{q^2})_1$ on a

$$A=\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)^{-1}=\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)$$

.

Ensuite comme ω_1 est un morphisme de groupe de $\mathbb{F}^*_{q^2}$ dans $\mathbb{C}^*$:
$0=\sum_{z\in\mathbb{F}^*_{q^2}}\omega_1(z)=\sum_{u\in\mathbb{F}^*_q}\sum_{z\in(\mathbb{F}^*_{q^2})_u}\omega_1(z)$
$=\sum_{u\in\mathbb{F}^*_q}\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(zz_u)$ pour tout $z_u\in(\mathbb{F}^*_{q^2})_u$
$=\sum_{u\in\mathbb{F}^*_q}\omega_1(z_u)\sum_{z\in(\mathbb{F}^*_{q^2})_1}\omega_1(z)$ pour tout $z_u\in(\mathbb{F}^*_{q^2})_u$
$=(\sum_{u\in\mathbb{F}^*_q}\omega_1(z_u))A$ pour tout $z_u\in(\mathbb{F}^*_{q^2})_u$
Donc soit $A=0$ et c'est fini, soit $\sum_{u\in\mathbb{F}^*_q}\omega_1(z_u)=0$ quelque soit le représentant z_u de $(\mathbb{F}^*_{q^2})_u$ pour tout u.
Notons $B_1,B_2,...,B_{q-1}$ les ensembles $(\mathbb{F}^*_{q^2})_u$ avec $u\in\mathbb{F}^*_q$.
Ainsi $\forall(z_1,...,z_{q-1})\in B_1\times\cdots\times B_{q-1}$, $\sum_{i=1}^{q-1}\omega_1(z_i)=0$.
En particulier en fixant $(z_2,...,z_{q-1})\in B_2\times\cdots\times B_{q-1}$ et en faisant varier z_1 dans $B_1=(\mathbb{F}^*_{q^2})_1$ on trouve que ω_1 est constant sur $(\mathbb{F}^*_{q^2})_1$ égale à $\omega_1(1)=1$. Or ceci est impossible car ω_1 est un morphisme de groupe de $\mathbb{F}^*_{q^2}$ dans $\mathbb{C}^*$ primitif, donc sa restriction à $(\mathbb{F}^*_{q^2})_1$ ne peut être triviale.

□

Pour montrer que $(\tilde{\rho}_{\omega_1},W_{\omega_1})$ et $(\tilde{\rho}_{\omega_2},W_{\omega_2})$ sont non isomorphes on va montrer que $\langle\chi_1,\chi_2\rangle=0$. Voici d'abord quelques petits résultats qui vont être utiles : ω_1 et ω_2 ainsi que ω_1 et $\omega_2\circ F$ sont non isomorphes donc par orthogonalité des caractères :

$$\sum_{a\in\mathbb{F}^*_{q^2}}\omega_1(a)\omega_2(a)=\sum_{a\in\mathbb{F}^*_{q^2}}\omega_1(a)(\omega_2\circ F)(a)=0.$$

Notons $P_1, ..., P_r$ les polynômes de degré 2 irréductibles dans $\mathbb{F}_q^*$. On a donc $r = \frac{q^2-q}{2}$. $\forall\ i \in [|1..r|]$ on choisit α_i une racine de P_i dans $\mathbb{F}_{q^2}^*$ et alors l'autre racine est $F(\alpha_i)$. De plus puisque $F \circ F = F$ on a que pour tout $i \neq j$, $\alpha_i \neq \alpha_j$ et $\alpha_i \neq F(\alpha_j)$. On a donc que $\{\alpha_1, F(\alpha_1), ..., \alpha_r, F(\alpha_r)\} = \mathbb{F}_{q^2}^* \backslash \mathbb{F}_q^*$.

Pour finir on rappelle que si $a \in \mathbb{F}_q^*$ on a $F(a) = a$.

En utilisant ces résultats et l'analyse des classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_q)$ on peut maintenant calculer $\langle \chi_1, \chi_2 \rangle$ et montrer que ce produit scalaire est nul :

$$\begin{aligned}
&\langle \chi_1, \chi_2 \rangle = \textstyle\sum_{a \in \mathbb{F}_q^*} ((q-1)\omega_1(a))((q-1)\omega_2(a)) \\
&+ \textstyle\sum_{a \in \mathbb{F}_q^*} (q-1)(q+1)(-\omega_1(a))(-\omega_2(a)) \\
&+ \textstyle\sum_{1 \leq i \leq r} q(q-1)(-\omega_1(\alpha_i) - \omega_1(F(\alpha_i)))(-\omega_2(\alpha_i) - \omega_2(F(\alpha_i))) \\
&= \textstyle\sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) + \sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) \\
&+ \textstyle\sum_{1 \leq i \leq r} q(q-1)(\omega_1(\alpha_i) + \omega_1(F(\alpha_i)))(\omega_2(\alpha_i) + \omega_2(F(\alpha_i))) \\
&= \textstyle\sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) + \sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) \\
&+ \textstyle\sum_{1 \leq i \leq r} q(q-1)\omega_1(\alpha_i)\omega_2(\alpha_i) + \sum_{1 \leq i \leq r} q(q-1)\omega_1(F(\alpha_i))\omega_2(F(\alpha_i)) \\
&+ \textstyle\sum_{1 \leq i \leq r} q(q-1)\omega_1(\alpha_i)\omega_2(F(\alpha_i)) + \sum_{1 \leq i \leq r} q(q-1)\omega_1(F(\alpha_i))\omega_2(\alpha_i) \\
&= \textstyle\sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) + \sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) \\
&+ \textstyle\sum_{a \in \mathbb{F}_{q^2}^* \backslash \mathbb{F}_q^*} q(q-1)\omega_1(a)\omega_2(a) + \sum_{1 \leq i \leq r} q(q-1)\omega_1(\alpha_i)(\omega_2 \circ F)(\alpha_i) \\
&+ \textstyle\sum_{1 \leq i \leq r} q(q-1)\omega_1(F(\alpha_i))(\omega_2 \circ F)(F(\alpha_i)) \\
&= \textstyle\sum_{a \in \mathbb{F}_{q^2}^*} q(q-1)\omega_1(a)\omega_2(a) + \sum_{a \in \mathbb{F}_q^*} q(q-1)\omega_1(a)(\omega_2 \circ F)(F(a)) \\
&+ \textstyle\sum_{a \in \mathbb{F}_{q^2}^* \backslash \mathbb{F}_q^*} q(q-1)\omega_1(a)(\omega_2 \circ F)(a) \\
&= q(q-1) \textstyle\sum_{a \in \mathbb{F}_{q^2}^*} \omega_1(a)\omega_2(a) + q(q-1) \sum_{a \in \mathbb{F}_{q^2}^*} \omega_1(a)(\omega_2 \circ F)(a) = 0.
\end{aligned}$$

□

Comme il y a exactement $q-1$ caractères non primitifs de $\mathbb{F}_{q^2}^*$ on a donc $q^2 - q$ caractères primitifs. Donc d'après la proposition précédente les $(\tilde{\rho}_\omega, W_\omega)$ nous donnent au moins $\frac{q^2-q}{2}$ représentations cuspidales irréductibles non isomorphes deux à deux. Or on sait qu'il y a exactement $\frac{q^2-q}{2}$ représentations cuspidales irréductibles non isomorphes deux à deux. Ce qui signifie qu'on les a toutes. De plus cela prouve la réciproque de la proposition précédente.

4.6.7 Bilan

Après les avoir construites voici un résumé de l'ensemble des représentations irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$ deux à deux non-isomorphes :

1. $q-1$ représentations irréductibles de degré 1,
2. $q-1$ représentations irréductibles de degré q,

3. $\frac{(q-1)(q-2)}{2}$ représentations irréductibles de degré $q+1$,
4. $\frac{q^2-q}{2}$ représentations irréductibles de degré $q-1$.

En sachant que pour chacune d'entre elles la partie 4 donne les moyens de construire explicitement ces représentations.

Références

[SIN] Anupam Singh, *Representation Theory of Finite Groups*, prépublication (1001.0462v1) sur arxiv.org.

[PRA] Amritanshu Prasad, *Représentations of* $\mathrm{GL}_2(\mathbb{F}_q)$ *and* $\mathrm{SL}_2(\mathbb{F}_q)$ *and some remarks about* $\mathrm{GL}_n(\mathbb{F}_q)$, prépublication (0712.4051v1) sur arxiv.org.

[JPS] Jean-Pierre Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, No. 42, Springer-Verlag, 1977.