

CARACTÈRES DU GROUPE LINÉAIRE DE RANG 2 SUR UN CORPS FINI

Dans ce chapitre, nous allons considérer le groupe linéaire $G = GL_2(\mathbf{F}_q)$ des matrices inversibles d'ordre 2×2 dont les entrées sont dans un corps fini \mathbf{F}_q ayant $q = p^e$ éléments, où p est un nombre premier, et déterminer sa table des caractères.

10.1 Rappelons que, pour toute puissance entière $q = p^e$ d'un nombre premier p , il existe un corps fini \mathbf{F}_q ayant q éléments. De plus, tout autre corps ayant q éléments est isomorphe à \mathbf{F}_q . Il est aussi bien connu que le groupe multiplicatif \mathbf{F}_q^\times d'un tel corps est un groupe cyclique, c'est-à-dire qu'il existe un élément $\zeta \in \mathbf{F}_q^\times$ tel que $\mathbf{F}_q^\times = \{\zeta^a \mid a = 0, 1, \dots, (q-2)\}$ et $\zeta^{q-1} = 1$.

Fixons un corps fini \mathbf{F}_q , où $q = p^e$ est une puissance entière de p ($e \in \{1, 2, 3, \dots\}$) et une clôture algébrique $\overline{\mathbf{F}}_q$ du corps \mathbf{F}_q . Nous noterons l'unique extension de degré 2 de \mathbf{F}_q contenue dans $\overline{\mathbf{F}}_q$ par \mathbf{F}_{q^2} . Alors $\mathbf{F}_{q^2} = \{x \in \overline{\mathbf{F}}_q \mid x^{q^2} = x\}$ et $\mathbf{F}_q = \{x \in \overline{\mathbf{F}}_q \mid x^q = x\} = \{x \in \mathbf{F}_{q^2} \mid x^q = x\}$. Fixons un générateur ξ du groupe cyclique $\mathbf{F}_{q^2}^\times$ tel que $\zeta = \xi^{q+1}$ est un générateur de \mathbf{F}_q^\times .

Notons par $\psi' : \mathbf{F}_{q^2}^\times \longrightarrow \mathbf{C}^\times$, un homomorphisme injectif de groupes. Par exemple, il suffit de prendre

$$\psi'(\xi^n) = \exp\left(\frac{2\pi n i}{q^2 - 1}\right), \quad 0 \leq n < (q^2 - 1).$$

Nous noterons par $\psi : \mathbf{F}_q^\times \longrightarrow \mathbf{C}^\times$, la restriction de ψ' au sous-groupe \mathbf{F}_q^\times de $\mathbf{F}_{q^2}^\times$. Si nous reprenons l'exemple ci-dessus, alors

$$\psi(\zeta^n) = \exp\left(\frac{2\pi n i}{q - 1}\right), \quad 0 \leq n < (q - 1).$$

Fixons aussi un caractère multiplicatif non-trivial $\omega : \mathbf{F}_q \longrightarrow \mathbf{C}^\times$ du groupe additif \mathbf{F}_q . Comme \mathbf{F}_q est un groupe abélien fini, nous avons vu au chapitre 4 comment déterminer tous les caractères multiplicatifs de tels groupes. Dans le cas présent, il y a ainsi q caractères multiplicatifs et il y a au moins un caractère multiplicatif non-trivial. Nous aurons besoin de $\omega : \mathbf{F}_q \longrightarrow \mathbf{C}^\times$ dans la construction de certains caractères induits. Pour nos calculs, ce qui est essentiel est que ω ne soit pas trivial.

Dans ce qui suivra, nous aurons à distinguer les cas où p est impair et pair.

Lemme 10.2 (a) Si p est un nombre premier impair, alors $(\mathbf{F}_q^\times)^2 = \{x^2 \mid x \in \mathbf{F}_q^\times\}$ est un sous-groupe de \mathbf{F}_q^\times d'indice 2.

(b) Si $p = 2$, alors $(\mathbf{F}_q^\times)^2 = \{x^2 \mid x \in \mathbf{F}_q^\times\} = \mathbf{F}_q^\times$.

(c) Si $p = 2$, alors la fonction $\mathbf{F}_q \longrightarrow \mathbf{F}_q$ définie par $x \mapsto x^2 + x$ est un homomorphisme de groupes additifs de noyau $\{0, 1\}$ et dont l'image $\{x^2 + x \mid x \in \mathbf{F}_q\}$ est un sous-groupe d'indice 2 dans \mathbf{F}_q .

Preuve: (a) Nous avons que $1 = 1^2 \in (\mathbf{F}_q^\times)^2$ et si $x^2, y^2 \in (\mathbf{F}_q^\times)^2$, alors $x^2(y^2)^{-1} = (xy^{-1})^2 \in (\mathbf{F}_q^\times)^2$. De ceci, nous pouvons conclure que $(\mathbf{F}_q^\times)^2$ est un sous-groupe de \mathbf{F}_q^\times . La fonction

$$\mathbf{Z}/(q-1)\mathbf{Z} \longrightarrow \mathbf{F}_q^\times \quad \text{définie par} \quad a + (q-1)\mathbf{Z} \longmapsto \zeta^a$$

est un isomorphisme et le sous-groupe $(\mathbf{F}_q^\times)^2$ correspond sous celui-ci au sous-groupe $2\mathbf{Z}/(q-1)\mathbf{Z}$. Noter que $(q-1)\mathbf{Z} \subseteq 2\mathbf{Z}$ parce que q est un entier impair. Donc $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

(b) Ceci est une simple conséquence du fait que $(q-1)$ et 2 sont premiers entre eux. En utilisant l'algorithme d'Euclide, nous obtenons que, pour tout $a + (q-1)\mathbf{Z} \in \mathbf{Z}/(q-1)\mathbf{Z}$, il existe un entier a' tel que $2a' + (q-1)\mathbf{Z} = a + (q-1)\mathbf{Z}$. En considérant notre argument en (a), nous pouvons conclure que $(\mathbf{F}_q^\times)^2 = \{x^2 \mid x \in \mathbf{F}_q^\times\} = \mathbf{F}_q^\times$.

(c) Parce que la caractéristique de \mathbf{F}_q est 2, alors nous avons

$$(x_1 + x_2)^2 + (x_1 + x_2) = x_1^2 + x_2^2 + x_1 + x_2 = (x_1^2 + x_1) + (x_2^2 + x_2)$$

et de ceci, nous obtenons que $x \mapsto x^2 + x$ est un homomorphisme de groupes additifs. Le noyau de cet homomorphisme est $\{x \in \mathbf{F}_q \mid x^2 + x = x(x+1) = 0\} = \{0, 1\}$. Nous obtenons alors facilement que l'image est un sous-groupe de \mathbf{F}_q de cardinalité $q/2$ et conséquemment d'indice 2

Lemme 10.3 (a) Si p est un nombre premier impair et $\Delta \in \mathbf{F}_q^\times \setminus (\mathbf{F}_q^\times)^2$, alors il existe $\delta \in \mathbf{F}_{q^2}^\times$ tel que $\delta^2 = \Delta$.

(b) Si $p = 2$ et $\Delta \in \mathbf{F}_q \setminus \{x^2 + x \mid x \in \mathbf{F}_q\}$, alors il existe $\delta \in \mathbf{F}_{q^2}^\times$ tel que $\delta^2 + \delta = \Delta$

Preuve: (a) Soit le générateur fixé ξ du groupe cyclique $\mathbf{F}_{q^2}^\times$. L'ordre de ξ est $q^2 - 1 = (q-1)(q+1)$. Il existe un entier a , $0 \leq a < (q^2 - 1)$, tel que $\Delta = \xi^a$. Nous avons que $\Delta^{q-1} = \xi^{a(q-1)} = 1$, car $\Delta \in \mathbf{F}_q^\times$. Alors $(q+1)$ divise a . Posons $a = (q+1)m$, où $m \in \mathbf{N}$. Nous obtenons que

$$\Delta = \xi^{m(q+1)} = \left(\xi^{\frac{m(q+1)}{2}} \right)^2. \quad \text{Il suffit de poser} \quad \delta = \xi^{\frac{m(q+1)}{2}}.$$

(b) Écrivons $\mathbf{F}_{q^2} = \mathbf{F}_q[\delta_1]$, où $\delta_1 \notin \mathbf{F}_q$. Nous avons que $\delta_1^2 = c + d\delta_1$, avec $d \neq 0$. En effet, si $d = 0$, alors $\delta_1^2 = c \in \mathbf{F}_q^\times$. Mais nous avons vu au lemme 10.2 (b) que les deux racines du polynôme $X^2 - c$ sont des éléments de \mathbf{F}_q et ceci contredit notre hypothèse que $\delta_1 \notin \mathbf{F}_q$.

Il existe un élément $\delta_2 \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ tel que $\delta_2^2 + \delta_2 \in \mathbf{F}_q \setminus \{x^2 + x \mid x \in \mathbf{F}_q\}$. En effet, il suffit de considérer $\delta_2 = d^{-1}\delta_1$. Alors $\delta_2^2 + \delta_2 = (d^{-1}\delta_1)^2 + (d^{-1}\delta_1) = d^{-2}\delta_1^2 + d^{-1}\delta_1 = d^{-2}(c + d\delta_1) + d^{-1}\delta_1 = cd^{-2} \in \mathbf{F}_q$. De plus $cd^{-2} \notin \{x^2 + x \mid x \in \mathbf{F}_q\}$, sinon, supposons que $cd^{-2} = x_1^2 + x_1$, alors les racines du polynôme $X^2 + X + cd^{-2}$ sont les éléments distincts x_1 et $x_1 + 1$ de \mathbf{F}_q , mais comme $\delta_2 \notin \mathbf{F}_q$ et δ_2 est une des racines, nous obtenons une contradiction. Posons $\Delta' = \delta_2^2 + \delta_2$.

Considérons maintenant $\Delta \in \mathbf{F}_q \setminus \{x^2 + x \mid x \in \mathbf{F}_q\}$. Alors, parce que $\{x^2 + x \mid x \in \mathbf{F}_q\}$ est un sous-groupe d'indice 2 de \mathbf{F}_q , nous avons que $\Delta + \Delta' \in \{x^2 + x \mid x \in \mathbf{F}_q\}$, i.e. il existe $a \in \mathbf{F}_q$ tel que $\Delta + \Delta' = a^2 + a$. Donc $\Delta = \Delta' + a^2 + a = \delta_2^2 + \delta_2 + a^2 + a = (\delta_2 + a)^2 + (\delta_2 + a)$. Il suffit de poser $\delta = \delta_2 + a \neq 0$ pour conclure la preuve de (b).

10.4 Si p est un nombre premier impair, fixons $\Delta \in \mathbf{F}_q^\times \setminus (\mathbf{F}_q^\times)^2$ et $\delta \in \mathbf{F}_{q^2}^\times$ tels que $\delta^2 = \Delta$; alors que, si $p = 2$, fixons $\Delta \in \mathbf{F}_q \setminus \{x^2 + x \mid x \in \mathbf{F}_q\}$ et $\delta \in \mathbf{F}_{q^2}^\times$ tels que $\delta^2 + \delta = \Delta$. Comme \mathbf{F}_{q^2} est de degré 2 sur \mathbf{F}_q , alors $\mathbf{F}_{q^2} = \mathbf{F}_q[\delta] = \{x + y\delta \mid x, y \in \mathbf{F}_q\}$. Il est bien connu que \mathbf{F}_{q^2} est une extension galoisienne de \mathbf{F}_q , dont le groupe de Galois a exactement 2 éléments. L'unique élément non trivial de ce groupe de Galois est

$$(\bar{\cdot}) : \mathbf{F}_{q^2} \longrightarrow \mathbf{F}_{q^2}, \quad \text{définie par} \quad z \longmapsto \bar{z} = z^q.$$

Si p est un nombre premier impair, alors, comme $\delta \notin \mathbf{F}_q$ et $\delta, -\delta$ sont les deux racines distinctes du polynôme $X^2 - \Delta \in \mathbf{F}_q[X]$, alors $\bar{\delta} = \delta^q = -\delta$ et $\overline{x + y\delta} = x - y\delta$ pour $x, y \in \mathbf{F}_q$.

Si $p = 2$, alors, comme $\delta \notin \mathbf{F}_q$ et $\delta, \delta+1$ sont les deux racines distinctes du polynôme $X^2 + X + \Delta \in \mathbf{F}_q[X]$, alors $\bar{\delta} = \delta^q = \delta + 1$ et $\overline{x + y\delta} = (x + y) + y\delta$ pour $x, y \in \mathbf{F}_q$.

Notation 10.5 Étant donné un élément $g \in GL_2(\mathbf{F}_q)$, alors nous noterons par $cl(g)$: la classe de conjugaison de g dans $GL_2(\mathbf{F}_q)$. Rappelons que la cardinalité $\#cl(g)$ de la classe de conjugaison de g est égale à $\#cl(g) = \#GL_2(\mathbf{F}_q)/\#Z(g)$, où $Z(g)$ est le centralisateur de g dans $GL_2(\mathbf{F}_q)$, c'est-à-dire que $Z(g) = \{g' \in GL_2(\mathbf{F}_q) \mid gg' = g'g\}$. Nous obtenons facilement que la cardinalité de $GL_2(\mathbf{F}_q)$ est $(q^2 - 1)(q^2 - q)$.

Notation 10.6 Nous allons définir des matrices inversibles de $GL_2(\mathbf{F}_q)$:

$$A(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, \quad \text{où } x \in \mathbf{F}_q^\times; \quad B(x) = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}, \quad \text{où } x \in \mathbf{F}_q^\times;$$

$$C(x, y) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \quad \text{où } x, y \in \mathbf{F}_q^\times, x \neq y;$$

$$D(z) = \begin{cases} \begin{pmatrix} x & y\Delta \\ y & x \end{pmatrix}, & \text{si } p \text{ est impair;} \\ \begin{pmatrix} x & y\Delta \\ y & (x+y) \end{pmatrix}, & \text{si } p = 2; \end{cases} \quad \text{où } z = x + y\delta \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times \text{ et } x, y \in \mathbf{F}_q$$

Lemme 10.7 Avec les notations ci-dessus, nous avons les résultats suivants.

(a) Le polynôme minimal de $A(x)$ est $X - x$ et la cardinalité $\#\text{cl}(A(x))$ de la classe de conjugaison $\text{cl}(A(x))$ est 1.

(b) Le polynôme minimal de $B(x)$ est $(X - x)^2$ et la cardinalité $\#\text{cl}(B(x))$ de la classe de conjugaison $\text{cl}(B(x))$ est $q^2 - 1 = (q - 1)(q + 1)$.

(c) Le polynôme minimal de $C(x, y)$ est $(X - x)(X - y)$ et la cardinalité $\#\text{cl}(C(x, y))$ de la classe de conjugaison $\text{cl}(C(x, y))$ est $q^2 + q = q(q + 1)$. De plus, les matrices $C(x, y)$ et $C(y, x)$ sont conjugués dans $GL_2(\mathbf{F}_q)$, c'est-à-dire $\text{cl}(C(x, y)) = \text{cl}(C(y, x))$.

(d) Le polynôme minimal de $D(z)$ est

$$(X - z)(X - \bar{z}) = \begin{cases} X^2 - 2xX + (x^2 - y^2\Delta), & \text{si } p \text{ est impair;} \\ X^2 + yX + (x^2 + xy + y^2\Delta), & \text{si } p = 2, \end{cases}$$

et la cardinalité $\#\text{cl}(D(z))$ de la classe de conjugaison $\text{cl}(D(z))$ est $q^2 - q = q(q - 1)$. De plus, les matrices $D(z)$ et $D(\bar{z})$ sont conjugués dans $GL_2(\mathbf{F}_q)$, c'est-à-dire $\text{cl}(D(z)) = \text{cl}(D(\bar{z}))$.

Preuve: (a) Il est clair que $(X - x)$ est le polynôme minimal de $A(x)$. De plus, comme $A(x)$ commute avec toutes les matrices de $GL_2(\mathbf{F}_q)$, alors le centralisateur de $A(x)$ dans $GL_2(\mathbf{F}_q)$ est $GL_2(\mathbf{F}_q)$ et $\#\text{cl}(A(x)) = 1$.

(b) Comme

$$\left[B(x) - x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad \left[B(x) - x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

alors $(X - x)^2$ est le polynôme minimal de $B(x)$. Si maintenant l'élément $g \in GL_2(\mathbf{F}_q)$ appartient au centralisateur de $B(x)$, alors g est de la forme

$$g = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \quad \text{avec } a \in \mathbf{F}_q^\times, b \in \mathbf{F}_q$$

et réciproquement toutes les matrices de cette forme sont dans le centralisateur de $B(x)$. Donc nous obtenons que $\#Z(B(x)) = q(q - 1)$ et $\#\text{cl}(B(x)) = (q^2 - 1) = (q - 1)(q + 1)$.

(c) Il est clair que $(X - x)(X - y)$ est le polynôme minimal de $C(x, y)$. Si maintenant l'élément $g \in GL_2(\mathbf{F}_q)$ appartient au centralisateur de $C(x, y)$, alors g est de la forme

$$g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \text{avec } a, d \in \mathbf{F}_q^\times$$

et réciproquement toutes les matrices de cette forme sont dans le centralisateur de $C(x, y)$. Donc nous obtenons que $\#Z(C(x, y)) = (q - 1)^2$ et $\#cl(C(x, y)) = (q^2 + q) = q(q + 1)$. De plus,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C(x, y) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C(x, y) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = C(y, x)$$

montre que les matrices $C(x, y)$ et $C(y, x)$ sont conjuguées

(d) Le polynôme

$$(X - z)(X - \bar{z}) = \begin{cases} X^2 - 2xX + (x^2 - y^2\Delta), & \text{si } p \text{ est impair;} \\ X^2 + yX + (x^2 + xy + y^2\Delta), & \text{si } p = 2, \end{cases}$$

est irréductible sur \mathbf{F}_q . En effet, les deux racines z et \bar{z} de ce polynôme sont deux éléments de $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Comme

$$(D(z))^2 - 2xD(z) + (x^2 - y^2\Delta) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

si p est impair et

$$(D(z))^2 + yD(z) + (x^2 + xy + y^2\Delta) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

si $p = 2$, nous obtenons que

$$(X - z)(X - \bar{z}) = \begin{cases} X^2 - 2xX + (x^2 - y^2\Delta), & \text{si } p \text{ est impair;} \\ X^2 + yX + (x^2 + xy + y^2\Delta), & \text{si } p = 2, \end{cases}$$

est le polynôme minimal de $D(z)$.

Si p est un nombre premier impair et supposons que l'élément $g \in GL_2(\mathbf{F}_q)$ appartient au centralisateur de $D(z)$, alors g est de la forme

$$g = \begin{pmatrix} a & c\Delta \\ c & a \end{pmatrix} \quad \text{avec } a, c \in \mathbf{F}_q \quad \text{tel que } a^2 - c^2\Delta \neq 0$$

et réciproquement toutes les matrices de cette forme sont dans le centralisateur de $D(z)$. Noter que $a^2 - c^2\Delta = 0$ si et seulement si $a = c = 0$ par notre choix de Δ . Donc nous obtenons que $\#Z(D(z)) = q^2 - 1$ et $\#cl(D(z)) = (q^2 - q) = q(q - 1)$. De plus,

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} D(z) \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} D(z) \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = D(\bar{z})$$

montre que les matrices $D(z)$ et $D(\bar{z})$ sont conjuguées

Si $p = 2$ et supposons que $g \in GL_2(\mathbf{F}_q)$ appartient au centralisateur de $D(z)$, alors g est de la forme

$$g = \begin{pmatrix} a & c\Delta \\ c & a + c \end{pmatrix} \quad \text{avec } a, c \in \mathbf{F}_q \quad \text{tel que } a^2 + ac + c^2\Delta \neq 0$$

et réciproquement toutes les matrices de cette forme sont dans le centralisateur de $D(z)$. Noter que $a^2 + ac + c^2\Delta = 0$ si et seulement si $a = c = 0$ par notre choix de Δ . Donc nous obtenons que $\#Z(D(z)) = (q^2 - 1)$ et $\#cl(D(z)) = (q^2 - q) = q(q - 1)$. De plus,

$$\begin{pmatrix} 0 & \Delta \\ 1 & 0 \end{pmatrix} D(z) \begin{pmatrix} 0 & \Delta \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \Delta \\ 1 & 0 \end{pmatrix} D(z) \begin{pmatrix} 0 & 1 \\ \Delta^{-1} & 0 \end{pmatrix} = D(\bar{z})$$

montre que les matrices $D(z)$ et $D(\bar{z})$ sont conjuguées

Proposition 10.8 Avec les notations du lemme 10.7, alors les classes de conjugaison de $GL_2(\mathbf{F}_q)$ sont $cl(A(x)), x \in \mathbf{F}_q^\times; cl(B(x)), x \in \mathbf{F}_q^\times; cl(C(x, y)) = cl(C(y, x)), x, y \in \mathbf{F}_q^\times, x \neq y; cl(D(z)) = cl(D(\bar{z})), z \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$ et nous avons le tableau suivant:

Classe $cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y)) = cl(C(y, x))$	$cl(D(z)) = cl(D(\bar{z}))$
$\#(cl(g))$	1	$(q^2 - 1)$	$(q^2 + q)$	$(q^2 - q)$
Nombre de classes	$(q - 1)$	$(q - 1)$	$(q - 1)(q - 2)/2$	$q(q - 1)/2$

En particulier, $GL_2(\mathbf{F}_q)$ a $(q - 1)(q + 1)$ classes de conjugaison.

Preuve: En considérant les polynômes minimaux des matrices $A(x)$, $B(x)$, $C(x, y)$ et $D(z)$ et parce que deux matrices conjuguées ont le même polynôme minimal, nous obtenons que toutes les classes de conjugaison $cl(A(x)), x \in \mathbf{F}_q^\times; cl(B(x)), x \in \mathbf{F}_q^\times; cl(C(x, y)) = cl(C(y, x)), x, y \in \mathbf{F}_q^\times, x \neq y; cl(D(z)) = cl(D(\bar{z})), z \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$ sont distinctes. Pour compléter, il suffit de vérifier qu'il ne manque pas de classes de conjugaison à notre liste. Mais si nous additionnons le nombre d'éléments de ces différentes classes, nous obtenons

$$(q - 1)(1) + (q - 1)(q^2 - 1) + \left(\frac{(q - 1)(q - 2)}{2}\right)(q^2 + q) + \left(\frac{q(q - 1)}{2}\right)(q^2 - q) = \#(GL_2(\mathbf{F}_q)).$$

De ceci, nous pouvons conclure qu'il ne manque pas de classes de conjugaison à notre liste. Le nombre de classes de conjugaison est alors

$$(q - 1) + (q - 1) + \frac{(q - 1)(q - 2)}{2} + \frac{q(q - 1)}{2} = (q - 1)(q + 1).$$

Avant de déterminer les caractères de degré 1 de $GL_2(\mathbf{F}_q)$, nous avons besoin d'un lemme sur les matrices g de $GL_2(\mathbf{F}_q)$ de déterminant $\det(g)$ égal à 1.

Lemme 10.9 Le sous-ensemble $SL_2(\mathbf{F}_q)$ des matrices g de $GL_2(\mathbf{F}_q)$ de déterminant $\det(g) = 1$ est un sous-groupe normal de $GL_2(\mathbf{F}_q)$ dont la cardinalité est $q(q^2 - 1) = q(q + 1)(q - 1)$. De plus, ce sous-groupe $SL_2(\mathbf{F}_q)$ est engendré par les matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \quad \text{où } x, y \in \mathbf{F}_q$$

Preuve: Comme $\det(gg') = \det(g)\det(g')$ et $\det(g^{-1}) = \det(g)^{-1}$ pour $g, g' \in GL_2(\mathbf{F}_q)$, nous obtenons facilement que $SL_2(\mathbf{F}_q)$ est un sous-groupe normal de $GL_2(\mathbf{F}_q)$.

Chaque matrice g de $GL_2(\mathbf{F}_q)$ peut s'écrire uniquement sous la forme

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \det g & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a/\det(g) & b/\det(g) \\ c & d \end{pmatrix} \quad \text{avec} \quad \begin{pmatrix} a/\det(g) & b/\det(g) \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_q)$$

Nous obtenons que $\#(GL_2(\mathbf{F}_q)) = (q - 1) \times \#(SL_2(\mathbf{F}_q))$ et ainsi $\#(SL_2(\mathbf{F}_q)) = (q^2 - 1)(q^2 - q)/(q - 1) = q(q^2 - 1)$

Il nous reste à montrer que $SL_2(\mathbf{F}_q)$ est engendré par les matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \quad \text{où } x, y \in \mathbf{F}_q.$$

Il suffit de noter premièrement les identités suivantes:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix};$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{si } a \neq 0;$$

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} \quad \text{si } a \neq 0.$$

Considérons une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_q), \quad \text{c'est-à-dire } ad - bc = 1.$$

Si $a \neq 0$, nous avons

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ac & 1 \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix} \quad \text{parce que } ad - bc = 1;$$

alors que, si $a = 0$, nous avons $b \neq 0$, $c \neq 0$ et

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix}$$

parce que $-bc = 1$. De tout ceci, nous obtenons le résultat.

Proposition 10.10 (a) Si $q > 2$, alors le sous-groupe dérivé de $GL_2(\mathbf{F}_q)$ est le sous-groupe $SL_2(\mathbf{F}_q)$ des matrices g de $GL_2(\mathbf{F}_q)$ de déterminant $\det(g)$ égal à 1. De plus, $GL_2(\mathbf{F}_q)$ a exactement $(q-1)$ caractères distincts de degré 1 et ceux-ci sont

$$\chi_1^{(m)} : GL_2(\mathbf{F}_q) \longrightarrow \mathbf{C}^\times, \quad g \longmapsto \chi_1^{(m)}(g) = [\psi(\det(g))]^m, \quad 0 \leq m < (q-1).$$

(b) Si $q = 2$, alors $GL_2(\mathbf{F}_2) = SL_2(\mathbf{F}_2)$ et $GL_2(\mathbf{F}_2)$ est isomorphe au groupe symétrique S_3 . Le sous-groupe dérivé de $GL_2(\mathbf{F}_2)$ est le sous-groupe

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

De plus, $GL_2(\mathbf{F}_2)$ a exactement 2 caractères distincts de degré 1 et ceux-ci sont premièrement le caractère trivial $\chi_1^{(0)} : GL_2(\mathbf{F}_q) \longrightarrow \mathbf{C}^\times$, $g \longmapsto \chi_1^{(0)}(g) = 1$ et deuxièmement le caractère $\chi_1^{(1)} : GL_2(\mathbf{F}_q) \longrightarrow \mathbf{C}^\times$ défini par

$$\chi_1^{(1)} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \chi_1^{(1)} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \chi_1^{(1)} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = 1 \quad \text{et} \quad \chi_1^{(1)} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \chi_1^{(1)} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \chi_1^{(1)} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$$

Preuve: (a) Il est facile de vérifier que $\chi_1^{(m)}$ est un caractère de degré 1 de $GL_2(\mathbf{F}_q)$, pour tout m , $0 \leq m < (q-1)$. Ceci est une conséquence du fait que $\det(gg') = \det(g)\det(g')$ pour $g, g' \in GL_2(\mathbf{F}_q)$, que ψ est un homomorphisme de groupes et finalement que la fonction $\mathbf{C}^\times \longrightarrow \mathbf{C}^\times$ définie par $z \longmapsto z^m$ est aussi un homomorphisme de groupes. Ces homomorphismes sont distincts parce que

$$\chi_1^{(m)} \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} = [\psi(\zeta)]^m = [\psi(\zeta)]^{m'} = \chi_1^{(m')} \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} \implies m = m',$$

où $0 \leq m, m' < (q-1)$. En effet, comme ψ est injectif, $\psi(\zeta)$ est une racine primitive complexe de 1 d'ordre $(q-1)$. De ceci, nous déduisons facilement que $m = m'$.

Pour terminer, il nous faut vérifier qu'il ne nous manque pas de caractères de degré 1. Nous avons vu au lemme 4.13 que ce nombre de caractères de degré 1 est l'indice du sous-groupe dérivé. Si nous montrons que le sous-groupe dérivé de $GL_2(\mathbf{F}_q)$ est $SL_2(\mathbf{F}_q)$, alors nous aurons que l'indice du sous-groupe dérivé dans $GL_2(\mathbf{F}_q)$ sera

$$\frac{\#(GL_2(\mathbf{F}_q))}{\#(SL_2(\mathbf{F}_q))} = \frac{(q^2-1)(q^2-q)}{(q^2-1)(q)} = (q-1).$$

Pour un commutateur $g_1 g_2 g_1^{-1} g_2^{-1}$ de $GL_2(\mathbf{F}_q)$, nous avons $\det(g_1 g_2 g_1^{-1} g_2^{-1}) = 1$. De ceci, nous pouvons déduire que le sous-groupe dérivé $D(GL_2(\mathbf{F}_q))$ de $GL_2(\mathbf{F}_q)$ est contenu dans $SL_2(\mathbf{F}_q)$. Comme nous avons vu au lemme précédent, $SL_2(\mathbf{F}_q)$ est engendré par les matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \quad \text{où } x, y \in \mathbf{F}_q.$$

Il suffit donc de montrer que chacune de ces matrices est un commutateur pour pouvoir conclure que $D(GL_2(\mathbf{F}_q)) = SL_2(\mathbf{F}_q)$. Soit un élément $w \in \mathbf{F}_q$, $w \neq 0, 1$. Alors nous obtenons ceci des expressions suivantes:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x/(w-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x/(w-1) \\ 0 & 1 \end{pmatrix}^{-1} \quad \text{pour } x \in \mathbf{F}_q$$

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y/(w-1) & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ y/(w-1) & 1 \end{pmatrix}^{-1} \quad \text{pour } y \in \mathbf{F}_q$$

Noter qu'ici nous utilisons le fait que $q > 2$ et qu'il existe alors un élément $w \in \mathbf{F}_q$, $w \neq 0, 1$.

(b) Nous avons que $\#(GL_2(\mathbf{F}_2)) = \#(SL_2(\mathbf{F}_2)) = 6$ et conséquemment $GL_2(\mathbf{F}_2) = SL_2(\mathbf{F}_2)$. Il est facile de voir qu'il y a exactement 3 droites vectorielles dans \mathbf{F}_2^2 , à savoir

$$L_0 = \mathbf{F}_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad L_1 = \mathbf{F}_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad L_\infty = \mathbf{F}_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

et les éléments de $GL_2(\mathbf{F}_2)$ permutent ces droites. Nous obtenons ainsi un homomorphisme de $GL_2(\mathbf{F}_2)$ avec S_3 et, par inspection, un isomorphisme. Les autres propriétés de la partie (b) de la proposition sont des simples conséquences de cet isomorphisme et de notre étude au chapitre 4. Nous avons déterminé au chapitre 4 (voir 4.10) la table des caractères de S_3 .

10.11 En résumé, si $q > 2$, alors les $(q-1)$ caractères irréductibles de degré 1 de $GL_2(\mathbf{F}_q)$ sont présentés dans le tableau suivant

Classe	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y)) = cl(C(y, x))$	$cl(D(z)) = cl(D(\bar{z}))$
$\chi_1^{(m)}(g)$	$[\psi(x)]^{2m}$	$[\psi(x)]^{2m}$	$[\psi(xy)]^m$	$[\psi(z\bar{z})]^m$

où $0 \leq m < (q-1)$.

Si $q = 2$, alors les 2 caractères irréductibles de degré 1 de $GL_2(\mathbf{F}_q)$ sont présentés dans le tableau suivant:

Classe	$cl(A(1))$	$cl(B(1))$	$cl(D(\delta)) = cl(D(\bar{\delta}))$
$\chi_1^{(0)}(g)$	1	1	1
$\chi_1^{(1)}(g)$	1	-1	1

Dans ce dernier cas, aucune matrice de $GL_2(\mathbf{F}_q)$ ne peut être conjuguée à une matrice de la forme $C(x, y)$ avec $x, y \in \mathbf{F}_q$ et $x \neq y$.

10.12 Nous allons maintenant considérer des caractères induits. Soient le sous-groupe B des matrices triangulaires supérieures de $G = GL_2(\mathbf{F}_q)$, le sous-groupe T des matrices diagonales de $GL_2(\mathbf{F}_q)$ et le sous-groupe U des matrices unipotentes de B , c'est-à-dire

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbf{F}_q, ad \neq 0 \right\}, \quad T = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbf{F}_q, ad \neq 0 \right\},$$

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{F}_q \right\}$$

Il est facile de vérifier que le sous-groupe T est isomorphe au produit direct $\mathbf{F}_q^\times \times \mathbf{F}_q^\times$ du groupe multiplicatif \mathbf{F}_q^\times avec lui-même et que le sous-groupe U est isomorphe au groupe additif \mathbf{F}_q . Nous avons aussi que $\#(B) = q(q-1)^2$, $\#(T) = (q-1)^2$ et $\#(U) = q$.

Étant donné deux entiers m, n tels que $0 \leq m, n < (q-1)$, nous pouvons considérer la fonction $\mu_{(m,n)}$ de B :

$$\mu_{(m,n)} : B \longrightarrow \mathbf{C}^\times \quad \text{définie par} \quad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \longmapsto \mu_{(m,n)} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = [\psi(a)]^m [\psi(d)]^n.$$

Cette fonction est un caractère multiplicatif de B . En effet, il est facile de vérifier

$$\mu_{(m,n)} \left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \right) = \mu_{(m,n)} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \mu_{(m,n)} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

10.13 Nous noterons par $\chi_{q+1}^{(m,n)}$: le caractère de la représentation induite $\text{Ind}_B^G(\mu_{(m,n)})$, où $0 \leq m, n < (q-1)$.

Il est nécessaire pour calculer le caractère $\chi_{q+1}^{(m,n)}$ d'étudier l'action de G sur G/B en réalisant G/B comme l'espace des droites vectorielles de \mathbf{F}_q^2 . Notons par $P(\mathbf{F}_q)$: l'espace projectif de \mathbf{F}_q^2 , c'est-à-dire $P(\mathbf{F}_q) = \{L \subset \mathbf{F}_q^2 \mid L \text{ sous-espace vectoriel de dimension 1}\}$. Nous convenons de noter les éléments de \mathbf{F}_q^2 comme des vecteurs colonnes. Nous noterons par $L_x, x \in \mathbf{F}_q$ et L_∞ les droites vectorielles suivantes:

$$L_x = \mathbf{F}_q \begin{pmatrix} 1 \\ x \end{pmatrix} \quad \text{pour } x \in \mathbf{F}_q \quad \text{et} \quad L_\infty = \mathbf{F}_q \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

et par $g_x, x \in \mathbf{F}_q$ et g_∞ les matrices de $GL_2(\mathbf{F}_q)$ suivantes:

$$g_x = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \quad \text{pour } x \in \mathbf{F}_q \quad \text{et} \quad g_\infty = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Lemme 10.14 (a) $P(\mathbf{F}_q) = \{L_x \mid x \in \mathbf{F}_q\} \cup \{L_\infty\}$ et la cardinalité de $P(\mathbf{F}_q)$ est $\#P(\mathbf{F}_q) = (q+1) = \#G/\#B$.

(b) $GL_2(\mathbf{F}_q)$ agit transitivement sur $P(\mathbf{F}_q)$ par $g \cdot L = g(L)$ et le stabilisateur de la droite vectorielle L_0 est B .

(c) La fonction $\tau : G/B \rightarrow P(\mathbf{F}_q)$, $gB \mapsto \tau(gB) = g(L_0)$ est bien définie et bijective. De plus, elle est G -équivariante, c'est-à-dire $\tau(gg'B) = g \cdot \tau(g'B)$ pour tout $g, g' \in G$. En particulier, $gg'B = g'B$ si et seulement si la droite vectorielle $\tau(g'B)$ est contenue dans un sous-espace propre dans \mathbf{F}_q^2 de la matrice $g \in G$.

(d) L'ensemble $X = \{g_x \mid x \in \mathbf{F}_q\} \cup \{g_\infty\}$ est un ensemble de représentants des classes à gauche de G suivant le sous-groupe B . De plus $g_x(L_0) = L_x$ pour $x \in \mathbf{F}_q$ et $g_\infty(L_0) = L_\infty$.

Preuve: (a) Soient une droite vectorielle L de \mathbf{F}_q^2 et un vecteur v non-nul de L . Alors nous avons que

$$v = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{cases} a \begin{pmatrix} 1 \\ a^{-1}b \end{pmatrix}, & \text{si } a \neq 0; \\ b \begin{pmatrix} 0 \\ 1 \end{pmatrix}, & \text{si } a = 0; \end{cases} \quad \text{et nous obtenons } L = \begin{cases} L_{a^{-1}b}, & \text{si } a \neq 0; \\ L_\infty, & \text{si } a = 0. \end{cases}$$

Donc $P(\mathbf{F}_q) = \{L_x \mid x \in \mathbf{F}_q\} \cup \{L_\infty\}$. Il est alors facile de calculer la cardinalité de $P(\mathbf{F}_q)$ comme étant $P(\mathbf{F}_q) = (q+1) = \#G/\#B$.

(b) Il est très facile de vérifier que $G \times P(\mathbf{F}_q) \rightarrow P(\mathbf{F}_q)$, $(g, L) \mapsto g \cdot L = g(L)$ est une action bien définie. Pour s'assurer qu'elle est transitive, il faut se rappeler le fait qu'une base d'un sous-espace V' d'un espace vectoriel V peut être complétée en une base de V . Si nous considérons deux droites vectorielles L et L' de \mathbf{F}_q^2 et deux bases $\mathcal{B} = \{v_1\}$, $\mathcal{B}' = \{v'_1\}$ de L et L' respectivement, alors nous pouvons compléter ces bases de L et L' en des bases de \mathbf{F}_q^2 : $\{v_1, v_2\}$ et $\{v'_1, v'_2\}$. Si nous considérons l'unique transformation linéaire $T : \mathbf{F}_q^2 \rightarrow \mathbf{F}_q^2$ telle que $T(v_1) = v'_1$ et $T(v_2) = v'_2$ et $g \in GL_2(\mathbf{F}_q)$, sa matrice associée (dans la base standard de \mathbf{F}_q^2), alors $g(L) = L'$. Ceci montre la transitivité.

Calculons le stabilisateur de la droite vectorielle L_0 . Nous avons

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} L_0 = L_0 \quad \Rightarrow \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \in L_0 \quad \Rightarrow \quad c = 0$$

et, de ceci, nous obtenons que le stabilisateur de L_0 est bien B .

(c) Le fait que la fonction τ est bien définie et bijective est une conséquence de (b). τ est G -équivariante, parce que $\tau(gg'B) = (gg') \cdot L_0 = g \cdot (g' \cdot L_0) = g \cdot \tau(g'B)$. Nous avons aussi que $gg'B = g'B$ si et seulement si $\tau(gg'B) = \tau(g'B)$ si et seulement si $g \cdot (\tau(g'B)) = g(\tau(g'B)) = \tau(g'B)$. Donc la droite vectorielle $\tau(g'B)$ est contenue dans un sous-espace propre de g dans \mathbf{F}_q^2 .

(d) Pour vérifier que X est l'ensemble de représentants des classes à gauche de G suivant le sous-groupe B , il suffit de noter que $g_x \cdot L_0 = L_x$ si $x \in \mathbf{F}_q$ et $g_\infty \cdot L_0 = L_\infty$. Ceci est facile à démontrer.

Théorème 10.15 (a) Les valeurs du caractère induit $\chi_{q+1}^{(m,n)}$ sur les classes de conjugaison sont données dans le tableau suivant:

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y))$	$cl(D(z))$
$\chi_{q+1}^{(m,n)}(g)$	$(q+1)[\psi(x)]^{m+n}$	$[\psi(x)]^{m+n}$	$[\psi(x)]^m[\psi(y)]^n + [\psi(y)]^m[\psi(x)]^n$	0

(b) $\chi_{q+1}^{(m,n)} = \chi_{q+1}^{(n,m)}$ pour tout $0 \leq m, n < (q-1)$.

(c) Si $0 \leq m \leq n < (q-1)$, $0 \leq m' \leq n' < (q-1)$ et $\chi_{q+1}^{(m,n)} = \chi_{q+1}^{(m',n')}$, alors $(m, n) = (m', n')$.

(d) Si $0 \leq m \leq n < (q-1)$, alors

$$\left(\chi_{q+1}^{(m,n)}, \chi_{q+1}^{(m,n)} \right)_{GL_2(\mathbf{F}_q)} = \begin{cases} 1, & \text{si } m \neq n; \\ 2, & \text{si } m = n. \end{cases}$$

En particulier, si $0 \leq m < n < (q-1)$, alors $\chi_{q+1}^{(m,n)}$ est un caractère irréductible de $GL_2(\mathbf{F}_q)$

(e) Si $0 \leq m < (q-1)$, alors

$$\left(\chi_{q+1}^{(m,m)}, \chi_1^{(m)} \right)_{GL_2(\mathbf{F}_q)} = 1$$

et $\chi_q^{(m)} = \chi_{q+1}^{(m,m)} - \chi_1^{(m)}$ est un caractère irréductible de $GL_2(\mathbf{F}_q)$.

(f) Si $0 \leq m < (q-1)$, alors les valeurs du caractère $\chi_q^{(m)}$ sur les classes de conjugaison sont données dans le tableau suivant:

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y))$	$cl(D(z))$
$\chi_q^{(m)}(g)$	$q[\psi(x)]^{2m}$	0	$[\psi(x) \psi(y)]^m$	$-[\psi(z\bar{z})]^m$

(g) Si $0 \leq m, m' < (q-1)$ et $\chi_q^{(m)} = \chi_q^{(m')}$, alors $m = m'$.

Preuve: (a) Pour calculer $\chi_{q+1}^{(m,n)}(g)$, il nous faut premièrement déterminer les sous-espaces propres de g dans \mathbf{F}_q^2 . Si $g = A(x)$ avec $x \in \mathbf{F}_q^\times$, alors $A(x)$ a une seule valeur propre: x et le sous-espace propre correspondant est \mathbf{F}_q^2 . Dans ce cas, nous avons $A(x)g' = g'A(x)$ si $g' \in X$, où $A(x) \in B$, et conséquemment $\chi_{q+1}^{(m,n)}(A(x)) = (q+1)[\psi(x)]^m[\psi(x)]^n$. Si $g = B(x)$ avec $x \in \mathbf{F}_q^\times$, alors $B(x)$ a une seule valeur propre: x et le sous-espace propre correspondant est L_0 . Dans ce cas, nous avons $B(x)g_0 = g_0B(x)$, où $B(x) \in B$, et conséquemment $\chi_{q+1}^{(m,n)}(B(x)) = [\psi(x)]^m[\psi(x)]^n$. Si $g = C(x, y)$ avec $x \neq y \in \mathbf{F}_q^\times$, alors $C(x, y)$ a deux valeurs propres distinctes: x et y . L'espace propre de $C(x, y)$ correspondant à x est L_0 et celui correspondant à y est L_∞ . Nous avons $C(x, y)g_0 = g_0C(x, y)$, où $C(x, y) \in B$, et $C(x, y)g_\infty = g_\infty C(y, x)$, où $C(y, x) \in B$, et conséquemment $\chi_{q+1}^{(m,n)}(C(x, y)) = [\psi(x)]^m[\psi(y)]^n + [\psi(y)]^m[\psi(x)]^n$. Si $g = D(z)$, où $z \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$, alors $D(z)$ a deux valeurs propres: z et \bar{z} . Comme celles-ci n'appartiennent pas à \mathbf{F}_q , il n'y a pas d'éléments de $P(\mathbf{F}_q)$ contenus dans un sous-espace propre sur \mathbf{F}_q . Conséquemment $\chi_{q+1}^{(m,n)}(D(z)) = 0$.

(b) De (a), nous obtenons que $\chi_{q+1}^{(m,n)} = \chi_{q+1}^{(n,m)}$.

(c) Si $0 \leq m \leq n < (q-1)$, $0 \leq m' \leq n' < (q-1)$ et $\chi_{q+1}^{(m,n)} = \chi_{q+1}^{(m',n')}$, alors nous voulons montrer que $(m, n) = (m', n')$. Rappelons que ζ est un générateur du groupe multiplicatif \mathbf{F}_q^\times et ψ est un homomorphisme injectif de \mathbf{F}_q^\times dans \mathbf{C}^\times . Donc $\psi(\zeta)$ est une racine primitive complexe de l'unité d'ordre $q-1$.

Si $m = n$, alors montrons que $m' = n'$. En effet, nous avons

$$\chi_{q+1}^{(m,n)}(C(\zeta, 1)) = 2[\psi(\zeta)]^m = [\psi(\zeta)]^{m'} + [\psi(\zeta)]^{n'} = \chi_{q+1}^{(m',n')}(C(\zeta, 1)) \Rightarrow 2 = [\psi(\zeta)]^{m'-m} + [\psi(\zeta)]^{n'-m}$$

et, en considérant la partie réelle de $[\psi(\zeta)]^{m'-m} + [\psi(\zeta)]^{n'-m}$, nous obtenons que $m' = n' = m$ et nous avons bien $(m, n) = (m', n')$. Nous pouvons donc supposer que $m < n$ et, par symétrie, que $m' < n'$. Sans perte de généralités, nous pouvons aussi supposer que $m \leq m'$.

Si $m = m'$, alors de

$$\chi_{q+1}^{(m,n)}(B(\zeta)) = [\psi(\zeta)]^{m+n} = [\psi(\zeta)]^{m'+n'} = \chi_{q+1}^{(m',n')}(B(\zeta)) \Rightarrow (m+n) \equiv (m'+n') \pmod{q-1}.$$

De ceci, nous pouvons conclure que $n \equiv n' \pmod{q-1}$ et, parce que $0 \leq n, n' < (q-1)$, nous obtenons $n = n'$ et $(m, n) = (m', n')$.

Nous pouvons donc supposer que $m \neq m'$. Nous avons donc $0 \leq m < n < (q-1)$, $0 \leq m' < n' < (q-1)$ et $m < m'$. À cause de ces inégalités, nous pouvons nous restreindre au cas où $q > 3$ et conséquemment $\zeta \neq \zeta^{-1}$. Nous allons montrer qu'il y a alors une contradiction avec le fait que $\chi_{q+1}^{(m,n)} = \chi_{q+1}^{(m',n')}$ lorsque nous supposons $0 \leq m < n < (q-1)$, $0 \leq m' < n' < (q-1)$ et $m < m'$.

Nous avons

$$\chi_{q+1}^{(m,n)}(C(\zeta, \zeta^{-1})) = [\psi(\zeta)]^{m-n} + [\psi(\zeta)]^{n-m} = [\psi(\zeta)]^{m'-n'} + [\psi(\zeta)]^{n'-m'} = \chi_{q+1}^{(m',n')}(C(\zeta, \zeta^{-1}))$$

et, de ceci, nous pouvons conclure que les parties réelles de $[\psi(\zeta)]^{n-m}$ et de $[\psi(\zeta)]^{n'-m'}$ sont égales. Nous avons soit $[\psi(\zeta)]^{n-m} = [\psi(\zeta)]^{n'-m'}$, soit $[\psi(\zeta)]^{n-m} = [\psi(\zeta)]^{m'-n'}$.

Rappelons que nous avons aussi

$$\chi_{q+1}^{(m,n)}(C(\zeta, 1)) = \chi_{q+1}^{(m',n')}(C(\zeta, 1)) \Rightarrow [\psi(\zeta)]^m + [\psi(\zeta)]^n = [\psi(\zeta)]^{m'} + [\psi(\zeta)]^{n'}. \quad (*)$$

Si $[\psi(\zeta)]^{n-m} = [\psi(\zeta)]^{n'-m'}$, alors $n - m = n' - m'$. De (*), nous obtenons

$$[\psi(\zeta)]^m (1 + [\psi(\zeta)]^{n-m}) = [\psi(\zeta)]^{m'} (1 + [\psi(\zeta)]^{n-m}) \Rightarrow \left([\psi(\zeta)]^{m'} - [\psi(\zeta)]^m \right) (1 + [\psi(\zeta)]^{n-m}) = 0.$$

Comme $0 \leq m < m' < (q-1)$, alors

$$\left([\psi(\zeta)]^{m'} - [\psi(\zeta)]^m \right) \neq 0 \quad \text{et} \quad (1 + [\psi(\zeta)]^{n-m}) = 0.$$

De ceci, nous pouvons conclure que p doit être impair et

$$n - m = n' - m' = \frac{q-1}{2} \Rightarrow n = m + \frac{q-1}{2} \quad \text{et} \quad n' = m' + \frac{q-1}{2}.$$

Nous obtenons ainsi que

$$(n + m) = 2m + \frac{q-1}{2} < 2m' + \frac{q-1}{2} = (n' + m').$$

Comme

$$\chi_{q+1}^{(m,n)}(B(\zeta)) = [\psi(\zeta)]^{m+n} = [\psi(\zeta)]^{m'+n'} = \chi_{q+1}^{(m',n')}(B(\zeta)) \Rightarrow (m+n) \equiv (m'+n') \pmod{q-1},$$

alors $m' + n' = m + n + (q-1)$ et

$$m' = m + \frac{q-1}{2} \Rightarrow n' = m + (q-1) \geq (q-1).$$

Cette dernière inégalité est absurde par nos hypothèses.

Si $[\psi(\zeta)]^{n-m} = [\psi(\zeta)]^{m'-n'}$, alors $n - m = m' - n' + (q-1)$. De (*), nous obtenons

$$[\psi(\zeta)]^m (1 + [\psi(\zeta)]^{n-m}) = [\psi(\zeta)]^{n'} (1 + [\psi(\zeta)]^{m'-n'}) \Rightarrow \left([\psi(\zeta)]^{n'} - [\psi(\zeta)]^m \right) (1 + [\psi(\zeta)]^{n-m}) = 0,$$

car $[\psi(\zeta)]^{m'-n'} = [\psi(\zeta)]^{n-m-(q-1)} = [\psi(\zeta)]^{n-m}$. Comme $0 \leq m < m' \leq n' < (q-1)$, alors

$$\left([\psi(\zeta)]^{n'} - [\psi(\zeta)]^m \right) \neq 0 \quad \text{et} \quad (1 + [\psi(\zeta)]^{n-m}) = 0.$$

De ceci, nous pouvons conclure que p doit être impair et

$$n - m = m' - n' + (q-1) = \frac{q-1}{2} \Rightarrow n = m + \frac{q-1}{2} \quad \text{et} \quad n' = m' + \frac{q-1}{2}.$$

Nous obtenons ainsi que

$$(n + m) = 2m + \frac{q-1}{2} < 2m' + \frac{q-1}{2} = (n' + m').$$

Comme

$$\chi_{q+1}^{(m,n)}(B(\zeta)) = [\psi(\zeta)]^{m+n} = [\psi(\zeta)]^{m'+n'} = \chi_{q+1}^{(m',n')}(B(\zeta)) \Rightarrow (m+n) \equiv (m'+n') \pmod{q-1},$$

alors $m' + n' = m + n + (q-1)$ et

$$m' = m + \frac{q-1}{2} \Rightarrow n' = m + (q-1) \geq (q-1).$$

Cette dernière inégalité est absurde par nos hypothèses.

(d) Nous allons calculer $(\chi_{q+1}^{(m,n)}, \chi_{q+1}^{(m,n)})_{GL_2(\mathbf{F}_q)}$ en utilisant le théorème de réciprocité de Frobenius (corollaire 6.12). Ainsi

$$(\chi_{q+1}^{(m,n)}, \chi_{q+1}^{(m,n)})_{GL_2(\mathbf{F}_q)} = (\chi_{q+1}^{(m,n)}, [\mu^{(m,n)} \uparrow_B^G])_{GL_2(\mathbf{F}_q)} = ([\chi_{q+1}^{(m,n)} \downarrow_B^G], \mu^{(m,n)})_B$$

Il nous suffit donc de déterminer le terme de droite de cette équation. Calculons premièrement les classes de conjugaison de B . Nous avons

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a' & (-a'b + ab' + bd')/d \\ 0 & d' \end{pmatrix}$$

dans B . De ceci, nous obtenons facilement que B a $q(q-1)$ classes de conjugaison et, en utilisant les notations de 9.6 (avec les mêmes conditions pour x et y), celles-ci sont énumérées dans le tableau suivant:

Classe $cl_B(g)$	$cl_B(A(x))$	$cl_B(B(x))$	$cl_B(C(x,y))$
$\#(cl_B(g))$	1	$(q-1)$	q
Nombre de classes	$(q-1)$	$(q-1)$	$(q-1)(q-2)$

Il suffit de procéder comme nous l'avons fait pour la proposition 10.8 en calculant le centralisateur de chacun des représentants des classes de conjugaison. Il faut noter ici que les matrices $C(x,y)$ et $C(y,x)$ ne sont pas conjuguées dans B lorsque $x, y \in \mathbf{F}_q^\times$ avec $x \neq y$. Il nous manque aucune classe de conjugaison, parce que $(q-1) + (q-1)^2 + q(q-1)(q-2) = q(q-1)^2 = \#B$. Nous obtenons donc

$$\begin{aligned} ([\chi_{q+1}^{(m,n)} \downarrow_B^G], \mu^{(m,n)})_B &= \frac{1}{q(q-1)^2} \left[\begin{aligned} &\sum_{x \in \mathbf{F}_q^\times} (q+1) [\psi(x)]^{m+n} \overline{[\psi(x)]^{m+n}} \\ &+ \sum_{x \in \mathbf{F}_q^\times} (q-1) [\psi(x)]^{m+n} \overline{[\psi(x)]^{m+n}} \\ &+ \sum_{x, y \in \mathbf{F}_q^\times, x \neq y} q \left[[\psi(x)]^m [\psi(y)]^n + [\psi(y)]^m [\psi(x)]^n \right] \overline{[\psi(x)]^m [\psi(y)]^n} \end{aligned} \right] \\ &= \frac{1}{q(q-1)^2} \left[\begin{aligned} &(q+1)(q-1) + (q-1)^2 + q(q-1)(q-2) \\ &+ q \sum_{x, y \in \mathbf{F}_q^\times, x \neq y} [\psi(x^{-1}y)]^m [\psi(xy^{-1})]^n \end{aligned} \right] \end{aligned}$$

Pour compléter la preuve de (d), il nous faut étudier

$$\sum_{x, y \in \mathbf{F}_q^\times, x \neq y} [\psi(x^{-1}y)]^m [\psi(xy^{-1})]^n = \sum_{x, y \in \mathbf{F}_q^\times, x \neq y} [\psi(xy^{-1})]^{n-m} \quad (\clubsuit)$$

Si nous utilisons la substitution $z = xy^{-1}$, nous obtenons que (\clubsuit) devient

$$\sum_{x, y \in \mathbf{F}_q^\times, x \neq y} [\psi(xy^{-1})]^{n-m} = \sum_{y, z \in \mathbf{F}_q^\times, z \neq e} [\psi(z)]^{n-m} = (q-1) \left(\sum_{z \in \mathbf{F}_q^\times} [\psi(z)]^{n-m} - 1 \right). \quad (\clubsuit')$$

Rappelons que $0 \leq m \leq n < (q-1)$. Si $m = n$, alors (\clubsuit') devient $(q-1)((q-1)-1) = (q-1)(q-2)$. Si $m < n$, alors

$$\sum_{z \in \mathbf{F}_q^\times} [\psi(z)]^{n-m} = \sum_{k=0}^{q-2} [\psi(\zeta)]^{k(n-m)} = \frac{[\psi(\zeta)]^{(n-m)(q-1)} - 1}{[\psi(\zeta)]^{n-m} - 1} = 0$$

car $[\psi(\zeta)]^{n-m} \neq 1$ et $[\psi(\zeta)]^{q-1} = 1$. De tout ceci, nous obtenons que si $m < n$, alors (\clubsuit') devient $-(q-1)$. Donc

$$\begin{aligned} \left([\chi_{q+1}^{(m,n)} \downarrow_B^G], \mu_{(m,n)} \right)_B &= \frac{1}{(q^3 - 2q^2 + q)} \left[q^3 - q^2 + \begin{cases} q(q-1)(q-2), & \text{si } m = n; \\ -q(q-1), & \text{si } m < n. \end{cases} \right] \\ &= \begin{cases} 2, & \text{si } m = n; \\ 1, & \text{si } m < n. \end{cases} \end{aligned}$$

Pour terminer la preuve, il suffit de noter que $\chi_{q+1}^{(m,n)}$ est irréductible lorsque $0 \leq m < n < (q-1)$, à cause de la proposition 3.2 et parce que $\chi_{q+1}^{(m,n)}$ est un caractère et $\left(\chi_{q+1}^{(m,n)}, \chi_{q+1}^{(m,n)} \right)_{GL_2(\mathbf{F}_q)} = 1$.

(e) Nous procédons comme nous l'avons fait en (d) en utilisant le théorème de réciprocity de Frobenius. Ainsi

$$\left(\chi_{q+1}^{(m,m)}, \chi_1^{(m)} \right)_{GL_2(\mathbf{F}_q)} = \left([\mu_{(m,m)} \uparrow_B^G], \chi_1^{(m)} \right)_{GL_2(\mathbf{F}_q)} = \left(\mu_{(m,m)}, [\chi_1^{(m)} \downarrow_B^G] \right)_B$$

Il nous suffit donc de déterminer le terme de droite de cette équation.

$$\begin{aligned} \left(\mu_{(m,m)}, [\chi_1^{(m)} \downarrow_B^G] \right)_B &= \frac{1}{q(q-1)^2} \left[\sum_{x \in \mathbf{F}_q^\times} [\psi(x)]^{2m} \overline{[\psi(x)]^{2m}} + \sum_{x \in \mathbf{F}_q^\times} (q-1) [\psi(x)]^{2m} \overline{[\psi(x)]^{2m}} \right] \\ &\quad + \sum_{x, y \in \mathbf{F}_q^\times, x \neq y} q [\psi(x)]^m \overline{[\psi(y)]^m} \overline{[\psi(x)]^m} [\psi(y)]^m \\ &= \frac{1}{q(q-1)^2} [(q-1) + (q-1)^2 + q(q-1)(q-2)] = 1 \end{aligned}$$

Comme $\left(\chi_{q+1}^{(m,m)}, \chi_1^{(m)} \right)_{GL_2(\mathbf{F}_q)} = 1$, alors $\chi_q^{(m)} = \chi_{q+1}^{(m,m)} - \chi_1^{(m)}$ est un caractère de $GL_2(\mathbf{F}_q)$. De plus comme $\left(\chi_{q+1}^{(m,m)}, \chi_{q+1}^{(m,m)} \right)_{GL_2(\mathbf{F}_q)} = 2$, nous obtenons par linéarité que $\left(\chi_q^{(m)}, \chi_q^{(m)} \right)_{GL_2(\mathbf{F}_q)} = 1$ et ainsi $\chi_q^{(m)}$ est irréductible.

(f) Les valeurs du caractère $\chi_q^{(m)} = \chi_{q+1}^{(m,m)} - \chi_1^{(m)}$ sont facilement obtenues de 10.11 et du théorème 10.15.

(g) Supposons que $0 \leq m, m' < (q-1)$ et $\chi_q^{(m)} = \chi_q^{(m')}$, alors nous voulons montrer que $m = m'$. Nous avons

$$\chi_q^{(m)}(C(\zeta, 1)) = [\psi(\zeta)]^m = [\psi(\zeta)]^{m'} = \chi_q^{(m')}(C(\zeta, 1)) \Rightarrow m = m',$$

parce que $\psi(\zeta)$ est une racine primitive complexe de l'unité d'ordre $(q-1)$.

10.16 Si nous résumons ce que nous avons obtenu jusqu'à maintenant, nous avons $(q-1)$ caractères irréductibles distincts de degré 1, $(q-1)(q-2)/2$ caractères irréductibles distincts de degré $(q+1)$ et $(q-1)$ caractères irréductibles distincts de degré q , soit au total

$$2(q-1) + \frac{(q-1)(q-2)}{2} = \frac{(q-1)(q+2)}{2}$$

caractères irréductibles. Comme il y a $(q-1)(q+1)$ classes de conjugaison dans $GL_2(\mathbf{F}_q)$, il nous manque encore

$$(q-1)(q+1) - \frac{(q-1)(q+2)}{2} = \frac{q(q-1)}{2}$$

caractères irréductibles, c'est-à-dire environ la moitié des caractères irréductibles.

10.17 Nous allons maintenant considérer des sous-groupes de $GL_2(\mathbf{F}_q)$ et induire de ceux-ci pour obtenir les caractères irréductibles manquants. Nous allons considérer une extension de notre notation présentée en 10.6.

Si $z = x + y\delta \in \mathbf{F}_{q^2}^\times$, où $x, y \in \mathbf{F}_q$, alors posons

$$D(z) = \begin{cases} \begin{pmatrix} x & y\Delta \\ y & x \end{pmatrix}, & \text{si } p \text{ est impair;} \\ \begin{pmatrix} x & y\Delta \\ y & (x+y) \end{pmatrix}, & \text{si } p = 2; \end{cases}$$

Il est facile de vérifier que $D(z) \in GL_2(\mathbf{F}_q)$ lorsque $z \in \mathbf{F}_{q^2}^\times$. En fait, la matrice $D(z)$ est celle associée à la transformation linéaire $z : \mathbf{F}_{q^2} \rightarrow \mathbf{F}_{q^2}$ définie par $z' \rightarrow zz'$ par rapport à la base $\{1, \delta\}$. De plus, $D(z)$ est diagonalisable pour tout $z \in \mathbf{F}_{q^2}^\times$. En effet, si $z \in \mathbf{F}_q^\times$, alors $D(z)$ est diagonale et a une seule valeur propre z avec multiplicité 2; alors que si $z \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$, $D(z)$ a deux valeurs propres distinctes: z et \bar{z} .

Lemma 10.18 *La fonction $D : \mathbf{F}_{q^2}^\times \rightarrow GL_2(\mathbf{F}_q)$ est un homomorphisme injectif de groupes.*

Preuve: Si $z_1 = x_1 + y_1\delta$, $z_2 = x_2 + y_2\delta \in \mathbf{F}_{q^2}^\times$, avec $x_1, x_2, y_1, y_2 \in \mathbf{F}_q$, alors il nous faut vérifier que $D(z_1z_2) = D(z_1)D(z_2)$. Si p est impair, nous avons que

$$D(z_1)D(z_2) = \begin{pmatrix} x_1 & y_1\Delta \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2\Delta \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} (x_1x_2 + y_1y_2\Delta) & (x_1y_2 + x_2y_1)\Delta \\ (x_1y_2 + x_2y_1) & (x_1x_2 + y_1y_2\Delta) \end{pmatrix} = D(z_1z_2),$$

car $z_1z_2 = (x_1 + y_1\delta)(x_2 + y_2\delta) = (x_1x_2 + y_1y_2\Delta) + (x_1y_2 + x_2y_1)\delta$. Rappelons que $\delta^2 = \Delta$. La fonction D est clairement injective.

Si p est pair, nous avons

$$\begin{aligned} D(z_1)D(z_2) &= \begin{pmatrix} x_1 & y_1\Delta \\ y_1 & (x_1 + y_1) \end{pmatrix} \begin{pmatrix} x_2 & y_2\Delta \\ y_2 & (x_2 + y_2) \end{pmatrix} \\ &= \begin{pmatrix} (x_1x_2 + y_1y_2\Delta) & (x_1y_2 + x_2y_1 + y_1y_2)\Delta \\ (x_1y_2 + x_2y_1 + y_1y_2) & (x_1x_2 + x_1y_2 + x_2y_1 + y_1y_2 + y_1y_2\Delta) \end{pmatrix} = D(z_1z_2), \end{aligned}$$

car $z_1z_2 = (x_1 + y_1\delta)(x_2 + y_2\delta) = (x_1x_2 + y_1y_2\Delta) + (x_1y_2 + x_2y_1 + y_1y_2)\delta$. Rappelons que $\delta^2 + \delta = \Delta$. La fonction D est clairement injective.

Notation 10.19 Posons

$$T' = \left\{ D(z) \in GL_2(\mathbf{F}_q) \mid z \in \mathbf{F}_{q^2}^\times \right\} \quad \text{et} \quad H = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbf{F}_q^\times, b \in \mathbf{F}_q \right\}$$

Lemma 10.20 (a) *T' est un sous-groupe de $GL_2(\mathbf{F}_q)$ isomorphe au groupe cyclique $\mathbf{F}_{q^2}^\times$. En particulier T' a $(q^2 - 1)$ éléments.*

(b) H est un sous-groupe de $GL_2(\mathbf{F}_q)$ ayant $q(q-1)$ éléments.

(c) Soit $m \in \mathbf{Z}$. Alors $\theta_m : T' \rightarrow \mathbf{C}^\times$ définie par $\theta_m(D(z)) = [\psi'(z)]^m$, où $z \in \mathbf{F}_{q^2}^\times$, est un caractère multiplicatif bien définie de T' .

(d) Soit $m \in \mathbf{Z}$. Alors $\eta_m : H \rightarrow \mathbf{C}^\times$ définie par

$$\eta_m \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = [\psi(a)]^m \omega(b/a), \quad \text{où } a \in \mathbf{F}_q^\times, b \in \mathbf{F}_q$$

est un caractère multiplicatif de H .

Preuve: (a) Nous avons vu au lemme 10.18 que D est un homomorphisme injectif de groupes. Comme T' est l'image de $\mathbf{F}_{q^2}^\times$ par D , le résultat est une conséquence facile de ce fait.

(b) Il est facile de vérifier que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H \quad \text{et} \quad \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix}^{-1} = \begin{pmatrix} a_1 a_2^{-1} & (a_2^{-1} b_1 - a_1 a_2^{-2} b_2) \\ 0 & a_1 a_2^{-1} \end{pmatrix} \in H.$$

De ceci, nous pouvons conclure que H est un sous-groupe de $GL_2(\mathbf{F}_q)$. Il y a $(q-1)$ choix possibles pour a et q choix possibles pour b . Conséquemment la cardinalité de H est $q(q-1)$.

(c) Comme D est une fonction injective, alors θ_m est bien définie. Si $z_1, z_2 \in \mathbf{F}_{q^2}^\times$, alors nous avons

$$\begin{aligned} \theta_m(D(z_1)D(z_2)) &= \theta_m(D(z_1 z_2)) = [\psi'(z_1 z_2)]^m = [\psi'(z_1)\psi'(z_2)]^m \\ &= [\psi'(z_1)]^m [\psi'(z_2)]^m = \theta_m(D(z_1))\theta_m(D(z_2)) \end{aligned}$$

parce que D et ψ' sont des homomorphismes de groupes.

(d) Si $a_1, a_2 \in \mathbf{F}_q^\times$ et $b_1, b_2 \in \mathbf{F}_q$, alors

$$\begin{aligned} \eta_m \left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \right) &= \eta_m \begin{pmatrix} a_1 a_2 & (a_1 b_2 + a_2 b_1) \\ 0 & a_1 a_2 \end{pmatrix} = [\psi(a_1 a_2)]^m \omega \left(\frac{a_1 b_2 + a_2 b_1}{a_1 a_2} \right) \\ &= [\psi(a_1)]^m [\psi(a_2)]^m \omega \left(\frac{b_1}{a_1} + \frac{b_2}{a_2} \right) = [\psi(a_1)]^m \omega \left(\frac{b_1}{a_1} \right) [\psi(a_2)]^m \omega \left(\frac{b_2}{a_2} \right) \\ &= \eta_m \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \eta_m \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix}. \end{aligned}$$

Nous avons utilisé le fait que ω est un caractère multiplicatif du groupe additif \mathbf{F}_q et que ψ est un caractère multiplicatif du groupe multiplicatif \mathbf{F}_q^\times . De ceci, nous pouvons conclure que η_m est un caractère multiplicatif de H .

Proposition 10.21 Soit $m \in \mathbf{Z}$. Considérons les représentations induites $Ind_{T'}^G(\theta_m)$ de la représentation θ_m du sous-groupe T' au groupe $GL_2(\mathbf{F}_q)$ et $Ind_H^G(\eta_m)$ de la représentation η_m du sous-groupe H au groupe $GL_2(\mathbf{F}_q)$. Notons respectivement les caractères induits correspondant par $[\theta_m \uparrow_{T'}^G]$ et par $[\eta_m \uparrow_H^G]$.

(a) Les valeurs des caractères induits $[\theta_m \uparrow_{T'}^G]$ et $[\eta_m \uparrow_H^G]$ sur les classes de conjugaison sont données dans le tableau suivant:

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y))$	$cl(D(z))$
$[\theta_m \uparrow_{T'}^G](g)$	$(q^2 - q)[\psi(x)]^m$	0	0	$[\psi'(z)]^m + \psi'(\bar{z})^m$
$[\eta_m \uparrow_H^G](g)$	$(q^2 - 1)[\psi(x)]^m$	$-[\psi(x)]^m$	0	0

(b) Nous avons

$$([\theta_m \uparrow_{T'}^G], [\theta_m \uparrow_{T'}^G])_{GL_2(\mathbf{F}_q)} = \begin{cases} (q-1), & \text{si } (q+1) \text{ ne divise pas } m; \\ q, & \text{si } (q+1) \text{ divise } m. \end{cases}$$

(c) Nous avons

$$([\eta_m \uparrow_H^G], [\eta_m \uparrow_H^G])_{GL_2(\mathbf{F}_q)} = q$$

(d) Nous avons

$$([\theta_m \uparrow_{T'}^G], [\eta_m \uparrow_H^G])_{GL_2(\mathbf{F}_q)} = (q-1)$$

Preuve: (a) Par la proposition 5.4, nous avons

$$[\theta_m \uparrow_{T'}^G](g) = \frac{1}{|T'|} \sum_{\substack{h \in G \\ h^{-1}gh \in T'}} \theta_m(h^{-1}gh).$$

Si $g = A(x)$, où $x \in \mathbf{F}_q^\times$, alors $g = D(x + 0\delta) \in T'$ et $h^{-1}gh = g$ pour tout $h \in G$. De ceci, nous obtenons que $\theta_m(h^{-1}gh) = \theta_m(g) = [\psi'(x)]^m = [\psi(x)]^m$ et

$$[\theta_m \uparrow_{T'}^G](A(x)) = \frac{|G|}{|T'|} [\psi(x)]^m = \frac{(q^2-1)(q^2-q)}{(q^2-1)} [\psi(x)]^m = (q^2-q)[\psi(x)]^m.$$

Si $g = B(x)$, où $x \in \mathbf{F}_q^\times$, alors g n'est pas diagonalisable sur $\overline{\mathbf{F}}_q$ et ceci reste valable pour toutes les matrices conjuguées $h^{-1}gh$, où $h \in GL_2(\mathbf{F}_q)$. Comme tous les éléments de T' sont diagonalisables, alors $h^{-1}gh \notin T'$ pour tout $h \in GL_2(\mathbf{F}_q)$ et

$$[\theta_m \uparrow_{T'}^G](B(x)) = 0.$$

Si $g = C(x, y)$, où $x, y \in \mathbf{F}_q^\times$ et $x \neq y$, alors g a deux valeurs propres distinctes x et y et celles-ci appartiennent toutes les deux à \mathbf{F}_q^\times . Les valeurs propres de $D(z)$ pour $z \in \mathbf{F}_{q^2}^\times$ sont distinctes si et seulement si $z \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$ et dans ce cas, elles sont égales à z et \bar{z} . Donc $h^{-1}gh \notin T'$ pour tout $h \in GL_2(\mathbf{F}_q)$ et

$$[\theta_m \uparrow_{T'}^G](C(x, y)) = 0.$$

Si $g = D(z)$, où $z = x + y\delta \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$ avec $x, y \in \mathbf{F}_q^\times$, alors les seules matrices $h^{-1}gh$ de g appartenant à T' sont $D(z)$ et $D(\bar{z})$ en considérant les valeurs propres de ces différentes matrices. Il nous faut donc déterminer toutes les matrices $h \in GL_2(\mathbf{F}_q)$ telles que $h^{-1}gh = D(z)$ et toutes celles $h \in GL_2(\mathbf{F}_q)$ telles que $h^{-1}gh = D(\bar{z})$.

Si p est impair et

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_q)$$

est telle que $h^{-1}gh = D(z)$ alors

$$\begin{pmatrix} x & y\Delta \\ y & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y\Delta \\ y & x \end{pmatrix}.$$

Parce que $y \neq 0$ et que $h \in GL_2(\mathbf{F}_q)$, nous obtenons facilement que $d = a$, $b = c\Delta$ et $(a, c) \neq (0, 0)$. La réciproque est aussi vraie. Ainsi

$$\{h \in GL_2(\mathbf{F}_q) \mid h^{-1}gh = D(z)\} = \left\{ h = \begin{pmatrix} a & c\Delta \\ c & a \end{pmatrix} \mid (a, c) \neq (0, 0) \right\}$$

et cet ensemble a $(q^2 - 1)$ éléments. Si p est impair et

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_q)$$

est telle que $h^{-1}gh = D(\bar{z})$ alors

$$\begin{pmatrix} x & y\Delta \\ y & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & -y\Delta \\ -y & x \end{pmatrix}.$$

Parce que $y \neq 0$ et que $h \in GL_2(\mathbf{F}_q)$, nous obtenons facilement que $d = -a$, $b = -c\Delta$ et $(a, c) \neq (0, 0)$. La réciproque est aussi vraie. Ainsi

$$\{h \in GL_2(\mathbf{F}_q) \mid h^{-1}gh = D(\bar{z})\} = \left\{ h = \begin{pmatrix} a & -c\Delta \\ c & -a \end{pmatrix} \mid (a, c) \neq (0, 0) \right\}$$

et cet ensemble a $(q^2 - 1)$ éléments.

Si p est pair et

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_q)$$

est telle que $h^{-1}gh = D(z)$ alors

$$\begin{pmatrix} x & y\Delta \\ y & (x+y) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y\Delta \\ y & (x+y) \end{pmatrix}.$$

Parce que $y \neq 0$ et que $h \in GL_2(\mathbf{F}_q)$, nous obtenons facilement que $d = (a + c)$, $b = c\Delta$ et $(a, c) \neq (0, 0)$. La réciproque est aussi vraie. Ainsi

$$\{h \in GL_2(\mathbf{F}_q) \mid h^{-1}gh = D(z)\} = \left\{ h = \begin{pmatrix} a & c\Delta \\ c & (a+c) \end{pmatrix} \mid (a, c) \neq (0, 0) \right\}$$

et cet ensemble a $(q^2 - 1)$ éléments. Si p est pair et

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_q)$$

est telle que $h^{-1}gh = D(\bar{z})$ alors

$$\begin{pmatrix} x & y\Delta \\ y & (x+y) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} (x+y) & y\Delta \\ y & x \end{pmatrix}.$$

Parce que $y \neq 0$ et que $h \in GL_2(\mathbf{F}_q)$, nous obtenons facilement que $d = a$, $b = a + c\Delta$ et $(a, c) \neq (0, 0)$. La réciproque est aussi vraie. Ainsi

$$\{h \in GL_2(\mathbf{F}_q) \mid h^{-1}gh = D(\bar{z})\} = \left\{ h = \begin{pmatrix} a & (a+c\Delta) \\ c & a \end{pmatrix} \mid (a, c) \neq (0, 0) \right\}$$

et cet ensemble a $(q^2 - 1)$ éléments.

De tout ceci, nous obtenons que

$$[\theta_m \uparrow_{T'}^G](D(z)) = \frac{1}{(q^2 - 1)} \left((q^2 - 1)\theta_m(D(z)) + (q^2 - 1)\theta_m(D(\bar{z})) \right) = [\psi'(z)]^m + [\psi'(\bar{z})]^m.$$

Nous avons ainsi calculé les valeurs du caractère $[\theta_m \uparrow_{T'}^G]$.

Calculons maintenant les valeurs du caractère $[\eta_m \uparrow_H^G]$. Par la proposition 5.4, nous avons

$$[\eta_m \uparrow_H^G](g) = \frac{1}{|H|} \sum_{\substack{h \in G \\ h^{-1}gh \in H}} \eta_m(h^{-1}gh).$$

Si $g = A(x)$, où $x \in \mathbf{F}_q^\times$, alors $g \in H$ et $h^{-1}gh = g$ pour tout $h \in G$. De ceci, nous obtenons que $\eta_m(h^{-1}gh) = \eta_m(g) = [\psi(x)]^m$ et

$$[\eta_m \uparrow_H^G](A(x)) = \frac{|G|}{|H|} [\psi(x)]^m = \frac{(q^2 - 1)(q^2 - q)}{q(q - 1)} [\psi(x)]^m = (q^2 - 1)[\psi(x)]^m.$$

Si $g = B(x)$, où $x \in \mathbf{F}_q^\times$, alors les seules matrices de H conjuguées (dans $GL_2(\overline{\mathbf{F}}_q)$) à g sont de la forme

$$\begin{pmatrix} x & b' \\ 0 & x \end{pmatrix} \quad \text{avec } b' \neq 0.$$

Il nous faut donc déterminer pour chaque $b' \in \mathbf{F}_q^\times$ l'ensemble des matrices

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_q) \text{ est telle que } \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & b' \\ 0 & x \end{pmatrix}.$$

Nous obtenons facilement que $c = 0$, $ab' = d$ et $a \neq 0$. Donc

$$\left\{ h \in GL_2(\mathbf{F}_q) \mid h^{-1}gh = \begin{pmatrix} x & b' \\ 0 & x \end{pmatrix} \right\} = \left\{ h = \begin{pmatrix} a & b \\ 0 & ab' \end{pmatrix} \mid a \in \mathbf{F}_q^\times, b \in \mathbf{F}_q \right\}$$

et cet ensemble a $q(q - 1)$ éléments. Nous avons aussi que

$$\eta_m \begin{pmatrix} x & b' \\ 0 & x \end{pmatrix} = [\psi(x)]^m \omega(b'/x).$$

Conséquemment

$$\begin{aligned} [\eta_m \uparrow_H^G](B(x)) &= \frac{1}{q(q - 1)} \sum_{b' \in \mathbf{F}_q^\times} q(q - 1) \eta_m \begin{pmatrix} x & b' \\ 0 & x \end{pmatrix} = \sum_{b' \in \mathbf{F}_q^\times} [\psi(x)]^m \omega(b'/x) \\ &= [\psi(x)]^m \sum_{b' \in \mathbf{F}_q^\times} \omega(b'/x) = [\psi(x)]^m \sum_{b'' \in \mathbf{F}_q^\times} \omega(b''), \end{aligned}$$

en utilisant la substitution $b'' = b'/x$ et en notant que la fonction $b' \rightarrow b'' = b'/x$ est une bijection du groupe multiplicatif \mathbf{F}_q^\times dans lui-même. Pour compléter notre calcul, il faut noter que

$$\sum_{b'' \in \mathbf{F}_q^\times} \omega(b'') = -1, \quad \text{car } \sum_{b'' \in \mathbf{F}_q} \omega(b'') = q(\omega, 1)_{\mathbf{F}_q} = 0 \quad \Rightarrow \quad \sum_{b'' \in \mathbf{F}_q^\times} \omega(b'') = -\omega(0) = -1$$

parce que ω n'est pas trivial. Finalement nous obtenons

$$[\eta_m \uparrow_H^G](B(x)) = -[\psi(x)]^m.$$

Si $g = C(x, y)$, où $x, y \in \mathbf{F}_q^\times$ et $x \neq y$ ou encore $g = D(z)$, où $z = x + y\delta \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$ avec $x, y \in \mathbf{F}_q^\times$, alors g n'est pas conjugué à aucun élément de H . Donc

$$[\eta_m \uparrow_H^G](C(x, y)) = 0 \quad \text{et} \quad [\eta_m \uparrow_H^G](D(z)) = 0$$

Ceci termine la preuve de (a).

(b) Par le théorème de réciprocité de Frobenius, plus précisément le corollaire 6.12, alors

$$\begin{aligned}
([\theta_m \uparrow_{T'}^G], [\theta_m \uparrow_{T'}^G])_{GL_2(\mathbf{F}_q)} &= ([[\theta_m \uparrow_{T'}^G] \downarrow_{T'}^G], \theta_m)_{T'} = \frac{1}{|T'|} \sum_{z \in \mathbf{F}_{q^2}^\times} [[\theta_m \uparrow_{T'}^G] \downarrow_{T'}^G](D(z)) \overline{\theta_m(D(z))} \\
&= \frac{1}{|T'|} \left[\sum_{x \in \mathbf{F}_q^\times} (q^2 - q) [\psi(x)]^m \overline{[\psi(x)]^m} + \sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} ([\psi'(z)]^m + [\psi'(z^q)]^m) \overline{[\psi'(z)]^m} \right] \\
&= \frac{1}{(q^2 - 1)} \left[(q^2 - q)(q - 1) + ((q^2 - 1) - (q - 1)) + \sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} [\psi'(z)]^{(q-1)m} \right] \\
&= \frac{1}{(q^2 - 1)} \left[q(q^2 - q) + \sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} [\psi'(z)]^{(q-1)m} \right].
\end{aligned}$$

Il nous faut donc calculer la somme

$$\sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} [\psi'(z)]^{(q-1)m}$$

en considérant soit que $(q + 1)$ ne divise pas m , soit que $(q + 1)$ divise m .

Si $(q + 1)$ ne divise pas m , alors $[\psi'(\xi)]^{(q-1)m} \neq 1$ et la somme recherchée devient alors

$$\sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} [\psi'(z)]^{(q-1)m} = \sum_{z \in \mathbf{F}_{q^2}^\times} [\psi'(z)]^{(q-1)m} - \sum_{x \in \mathbf{F}_q^\times} [\psi(x)]^{(q-1)m} = \frac{[\psi'(\xi)]^{(q-1)m(q^2-1)} - 1}{[\psi'(\xi)]^{(q-1)m} - 1} - (q - 1) = -(q - 1)$$

car $[\psi(x)]^{(q-1)} = 1$ et $[\psi'(\xi)]^{(q-1)m(q^2-1)} = 1$.

Si $(q + 1)$ divise m , alors $[\psi'(\xi)]^{(q-1)m} = 1$ et la somme recherchée devient alors

$$\sum_{\substack{z \in \mathbf{F}_{q^2}^\times \\ z \notin \mathbf{F}_q^\times}} [\psi'(z)]^{(q-1)m} = ((q^2 - 1) - (q - 1)) = (q^2 - q).$$

De tout ceci, nous obtenons facilement que

$$([\theta_m \uparrow_{T'}^G], [\theta_m \uparrow_{T'}^G])_{GL_2(\mathbf{F}_q)} = \begin{cases} (q - 1), & \text{si } (q + 1) \text{ ne divise pas } m; \\ q, & \text{si } (q + 1) \text{ divise } m. \end{cases}$$

(c) Par le théorème de réciprocité de Frobenius, plus précisément le corollaire 6.12, alors

$$\begin{aligned}
([\eta_m \uparrow_H^G], [\eta_m \uparrow_H^G])_{GL_2(\mathbf{F}_q)} &= ([[\eta_m \uparrow_H^G] \downarrow_H^G], \eta_m)_H \\
&= \frac{1}{q(q - 1)} \left[\sum_{x \in \mathbf{F}_q^\times} (q^2 - 1) [\psi(x)]^m \overline{[\psi(x)]^m} + \sum_{x, y \in \mathbf{F}_q^\times} (-1) [\psi(x)]^m \overline{[\psi(x)]^m} \omega(y/x) \right] \\
&= \frac{1}{q(q - 1)} \left[(q^2 - 1)(q - 1) - \sum_{x, y \in \mathbf{F}_q^\times} \overline{\omega(y/x)} \right].
\end{aligned}$$

Mais comme nous l'avons vu en (a), nous obtenons pour chaque $x \in \mathbf{F}_q^\times$ que

$$\sum_{y \in \mathbf{F}_q^\times} \overline{\omega(y/x)} = \overline{\sum_{y \in \mathbf{F}_q^\times} \omega(y/x)} = -1.$$

Donc

$$([\eta_m \uparrow_H^G], [\eta_m \uparrow_H^G])_{GL_2(\mathbf{F}_q)} = \frac{1}{q(q-1)} [(q^2-1)(q-1) + (q-1)] = q.$$

(d) Par le théorème de réciprocité de Frobenius, plus précisément le corollaire 6.12, alors

$$\begin{aligned} ([\theta_m \uparrow_{T'}^G], [\eta_m \uparrow_H^G])_{GL_2(\mathbf{F}_q)} &= ([[\theta_m \uparrow_{T'}^G] \downarrow_H^G], \eta_m)_H = \frac{1}{q(q-1)} \sum_{x \in \mathbf{F}_q^\times} (q^2 - q)[\psi(x)]^m \overline{[\psi(x)]^m} \\ &= \frac{(q^2 - q)(q-1)}{q(q-1)} = (q-1) \end{aligned}$$

car $\theta_m(B(x)) = 0$ pour tout $x \in \mathbf{F}_q^\times$.

Notation 10.22 Soit un entier $m \in \mathbf{N}$ tel que $0 \leq m < (q^2 - 1)$ et $(q+1)$ ne divise pas m , alors le caractère généralisé $[\eta_m \uparrow_H^G] - [\theta_m \uparrow_{T'}^G]$ de $GL_2(\mathbf{F}_q)$ sera noté $\chi_{q-1}^{(m)}$. Rappelons que nous avons défini en 7.20 la notion de caractère généralisé.

Théorème 10.23 (a) Soit un entier $m \in \mathbf{N}$ tel que $0 \leq m < (q^2 - 1)$ et $(q+1)$ ne divise pas m , alors le caractère généralisé $\chi_{q-1}^{(m)}$ est un caractère irréductible et les valeurs de $\chi_{q-1}^{(m)}$ sur les classes de conjugaison sont données dans le tableau suivant

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y))$	$cl(D(z))$
$\chi_{q-1}^{(m)}(g)$	$(q-1)[\psi(x)]^m$	$-[\psi(x)]^m$	0	$-([\psi'(z)]^m + [\psi'(\bar{z})]^m)$

(b) Soient deux entiers $m, m' \in \mathbf{N}$ distincts tels que $0 \leq m \neq m' < (q^2 - 1)$ et $(q+1)$ ne divise pas m et m' . Alors $\chi_{q-1}^{(m')} = \chi_{q-1}^{(m)}$ si et seulement si $m' \equiv qm \pmod{q^2 - 1}$.

Preuve: (a) Les valeurs de $\chi_{q-1}^{(m)}$ sur les classes de conjugaison sont facilement obtenues de la proposition 10.21. Pour compléter la preuve de (a), il suffit de vérifier à cause du lemme 7.21 que $\chi_{q-1}^{(m)}(A(1)) > 0$ et que $(\chi_{q-1}^{(m)}, \chi_{q-1}^{(m)})_{GL_2(\mathbf{F}_q)} = 1$ et, de ceci, nous pourrions conclure que $\chi_{q-1}^{(m)}$ est un caractère irréductible. En effet, nous avons $\chi_{q-1}^{(m)}(A(1)) = (q-1) > 0$, ainsi que

$$\begin{aligned} (\chi_{q-1}^{(m)}, \chi_{q-1}^{(m)})_{GL_2(\mathbf{F}_q)} &= ([\eta_m \uparrow_H^G] - [\theta_m \uparrow_{T'}^G], [\eta_m \uparrow_H^G] - [\theta_m \uparrow_{T'}^G])_{GL_2(\mathbf{F}_q)} \\ &= ([\eta_m \uparrow_H^G], [\eta_m \uparrow_H^G])_G - 2([\eta_m \uparrow_H^G], [\theta_m \uparrow_{T'}^G])_G + ([\theta_m \uparrow_{T'}^G], [\theta_m \uparrow_{T'}^G])_G \\ &= q - 2(q-1) + (q-1) = 1 \end{aligned}$$

parce que $(q+1)$ ne divise pas m .

(b) Il est facile de vérifier que $\chi_{q-1}^{(m')} = \chi_{q-1}^{(m)}$ lorsque $m' \equiv qm \pmod{q^2 - 1}$. Supposons maintenant que $\chi_{q-1}^{(m')} = \chi_{q-1}^{(m)}$ et montrons que $m' \equiv qm \pmod{q^2 - 1}$. Comme $\chi_{q-1}^{(m)}(B(\zeta)) = -[\psi(\zeta)]^m = -[\psi(\zeta)]^{m'} = \chi_{q-1}^{(m')}(B(\zeta))$, nous avons $[\psi(\zeta)]^m = [\psi'(\xi)]^{(q+1)m} = [\psi'(\xi)]^{(q+1)m'} = [\psi(\zeta)]^{m'}$ par nos choix de ζ et de ξ . Nous noterons l'élément $[\psi(\zeta)]^m = [\psi(\zeta)]^{m'}$ par κ . Aussi de

$$\chi_{q-1}^{(m)}(D(\xi)) = -([\psi'(\xi)]^m + [\psi'(\xi)]^{qm}) = -([\psi'(\xi)]^{m'} + [\psi'(\xi)]^{qm'}) = \chi_{q-1}^{(m')}(D(\xi)),$$

nous obtenons que $[\psi'(\xi)]^m + [\psi'(\xi)]^{qm} = [\psi'(\xi)]^{m'} + [\psi'(\xi)]^{qm'}$. Ainsi

$$\begin{aligned} [\psi'(\xi)]^m + [\psi'(\xi)]^{(q+1)m}[\psi'(\xi)]^{-m} &= [\psi'(\xi)]^m + \kappa [\psi'(\xi)]^{-m} = [\psi'(\xi)]^{m'} + \kappa [\psi'(\xi)]^{-m'} \\ &= [\psi'(\xi)]^{m'} + [\psi'(\xi)]^{(q+1)m'}[\psi'(\xi)]^{-m'} \end{aligned}$$

et ainsi

$$[\psi'(\xi)]^m - [\psi'(\xi)]^{m'} = \kappa \left(\frac{1}{[\psi'(\xi)]^{m'}} - \frac{1}{[\psi'(\xi)]^m} \right) = \kappa \left(\frac{[\psi'(\xi)]^m - [\psi'(\xi)]^{m'}}{[\psi'(\xi)]^{m+m'}} \right).$$

Par nos hypothèses sur m et m' , nous avons que $[\psi'(\xi)]^m - [\psi'(\xi)]^{m'} \neq 0$. Nous pouvons donc conclure que $[\psi'(\xi)]^{m+m'} = \kappa = [\psi'(\xi)]^{(q+1)m} \Rightarrow m + m' \equiv (q+1)m \pmod{q^2-1} \Rightarrow m' \equiv qm \pmod{q^2-1}$.

Remarque 10.24 Pour chaque paire d'entiers distincts $\{m, m'\}$ avec $0 \leq m \neq m' < (q^2 - 1)$ et $(q+1)$ ne divise pas m et m' , alors nous obtenons un caractère irréductible $\chi_{q-1}^{(m)} = \chi_{q-1}^{(m')}$ de $GL_2(\mathbf{F}_q)$ et pour une autre paire d'entiers distincts $\{m_1, m'_1\} \neq \{m, m'\}$ avec $0 \leq m_1 \neq m'_1 < (q^2 - 1)$ et $(q+1)$ ne divise pas m_1 et m'_1 , alors $\chi_{q-1}^{(m_1)} \neq \chi_{q-1}^{(m'_1)}$. Donc le nombre de caractères irréductibles de degré $(q-1)$ de $GL_2(\mathbf{F}_q)$ obtenus au théorème 10.23 est

$$\frac{1}{2} \left((q^2 - 1) - \frac{(q^2 - 1)}{(q+1)} \right) = \frac{q^2 - q}{2}$$

Suite à 10.16, nous avons ainsi obtenu tous les caractères irréductibles de $GL_2(\mathbf{F}_q)$.

10.25 En résumé, si $q > 2$, alors la table de caractères de $GL_2(\mathbf{F}_q)$ est

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x, y))$
$\chi_1^{(m)}(g)$	$[\psi(x)]^{2m}$	$[\psi(x)]^{2m}$	$[\psi(xy)]^m$
$\chi_{q+1}^{(m,n)}(g)$	$(q+1)[\psi(x)]^{m+n}$	$[\psi(x)]^{m+n}$	$[\psi(x)]^m[\psi(y)]^n + [\psi(y)]^m[\psi(x)]^n$
$\chi_q^{(m)}(g)$	$q[\psi(x)]^{2m}$	0	$[\psi(x) \ \psi(y)]^m$
$\chi_{q-1}^{(m)}(g)$	$(q-1)[\psi(x)]^m$	$-\psi(x)^m$	0

$cl(g)$	$cl(D(z))$
$\chi_1^{(m)}(g)$	$[\psi(z\bar{z})]^m$
$\chi_{q+1}^{(m,n)}(g)$	0
$\chi_q^{(m)}(g)$	$-\psi(z\bar{z})^m$
$\chi_{q-1}^{(m)}(g)$	$-(\psi'(z))^m + (\psi'(\bar{z}))^m$

Dans cette table, les colonnes sont indexés par les classes des matrices: $A(x)$ pour chaque $x \in \mathbf{F}_q^\times$; $B(x)$ pour chaque $x \in \mathbf{F}_q^\times$; $C(x, y)$ pour chaque paire $\{x, y\} \subset \mathbf{F}_q^\times$, $x \neq y$; $D(z)$ pour chaque paire $\{z, \bar{z}\} \subset \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$. Les lignes sont indexées par les caractères: $\chi_1^{(m)}$ pour $0 \leq m < (q-1)$; $\chi_{q+1}^{(m,n)}$ pour $0 \leq m < n < (q-1)$; $\chi_q^{(m)}$ pour $0 \leq m < (q-1)$; $\chi_{q-1}^{(m)}$ pour chaque paire $\{m + (q^2 - 1)\mathbf{Z}, qm + (q^2 - 1)\mathbf{Z}\} \subset \mathbf{Z}/(q^2 - 1)\mathbf{Z}$ telle que $0 \leq m < (q^2 - 1)$ et $(q+1)$ ne divise pas m .

Si $q = 2$, alors $GL_2(\mathbf{F}_2)$ est isomorphe au groupe symétrique S_3 et sa table de caractère a été déterminée au chapitre 4 (voir 4.10).

Remarque 10.26. Les caractères $\chi_1^{(m)}$, $\chi_{q+1}^{(m,n)}$ et $\chi_q^{(m)}$ sont dits être dans la série principale, c'est-à-dire qu'ils apparaissent dans les caractères induits $[\mu_{(m,n)} \uparrow_B^G]$. Les caractères $\chi_{q-1}^{(m)}$ sont dits être dans la série discrète, c'est-à-dire qu'ils n'apparaissent dans aucun des caractères induits $[\mu_{(m,n)} \uparrow_B^G]$.

Le caractère $\chi_q^{(0)}$ est appelé le caractère de Steinberg. Les valeurs de $\chi_q^{(0)}$ sur les classes de conjugaison sont données dans le tableau suivant

$cl(g)$	$cl(A(x))$	$cl(B(x))$	$cl(C(x,y))$	$cl(D(z))$
$\chi_q^{(0)}(g)$	q	0	1	-1

Ainsi ce caractère est de degré: la plus grande puissance de p divisant $\#(GL_2(\mathbf{F}_q))$ et il s'annule pour les matrices qui ne sont pas diagonalisables sur $\overline{\mathbf{F}}_q$, c'est-à-dire celles de la classe $cl(B(x))$. C'est un exemple d'un caractère unipotent. Il y a deux caractères unipotents pour $GL_2(\mathbf{F}_q)$, un pour chaque partage de 2: $\chi_1^{(0)}$ et $\chi_q^{(0)}$. Le caractère de Steinberg $\chi_q^{(0)}$ joue un rôle similaire pour le groupe linéaire au caractère signe pour le groupe symétrique.