CLASSES DE CONJUGAISON DE $\mathrm{GL}_2(F), \mathrm{SL}_2(F)$ ET $\mathrm{PSL}_2(F)$

GRÉGORY BERHUY

Le but de cet article est de déterminer les classes de conjugaison des groupes $\mathrm{GL}_2(F), \mathrm{SL}_2(F)$ et $\mathrm{PSL}_2(F)$, d'abord lorsque F un corps quelconque, puis lorsque F est un corps fini. Dans ce dernier cas, on calculera également le nombre de classes de conjugaison et leurs cardinaux, ainsi qu'un système complet de représentants de classes de conjugaison.

1. Échauffement: classes de conjugaison de $\mathrm{GL}_2(F)$

On commence par le cas plus facile. Ici, F désignera un corps quelconque.

Deux matrices conjuguées ayant le même polynome minimal, on voit qu'une matrice $M \in \mathrm{GL}_2(F)$ peut être de quatre types distincts:

(1) Type I: $\mu_M = X - \lambda$, avec $\lambda \in F^\times$.

(2) Type II: $\mu_M = (X - \lambda_1)(X - \lambda_2)$, avec $\lambda_1, \lambda_2 \in F^\times$ distincts.

(3) Type III: $\mu_M = (X - \lambda)^2$, avec $\lambda \in F^\times$.

(4) Type IV: μ_M est irréductible sur F, de degré 2.

Par définition, une matrice possède un unique type, et deux matrices de types différents ne peuvent être conjuguées. Analysons maintenant chaque cas.

Soit $M \in \mathrm{GL}_2(F)$.

Si M est de type I, elle est diagonalisable, et semblable à λI_2, avec $\lambda \in F^\times$.

Si M est de type II, elle est diagonalisable, et semblable à $\begin{pmatrix} \lambda_1 & 0 \\ & \lambda_2 \end{pmatrix}$.

Si M est de type III, soit $e_1 \in F^2$ un vecteur propre associé à λ, que l'on complète en une base $\mathscr{B} = (e_1, e_2)$ de F^2. Si P est la matrice de $\mathscr{B}$ dans la base canonique, on a donc

$$P^{-1}MP = \begin{pmatrix} \lambda & b \\ 0 & d \end{pmatrix},$$

avec $b, d \in F$. Comme cette dernière matrice est triangulaire, ses coefficients diagonaux sont les valeurs propres de M, et par conséquent, $d = \lambda$. Notons que b est non nul, puisque M n'est pas diagonalisable. Mais alors, l'égalité

$$\begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & b \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

montre que M est semblable à $T(\lambda) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$.

Supposons enfin que $\mu_M = X^2 - tX + d \in F[X]$ n'ait pas de racines dans F. Comme $\mu_M \mid \chi_M$, on a $\chi_M = \mu_M$.

Notons que M ne peut être triangulaire, car sinon χ_M serait scindé. Ainsi, si $\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et la première colonne de M, c'est-à-dire $M\varepsilon_1$, ne sont pas proportionnels. Autrement dit, $\mathscr{B} = (\varepsilon_1, M\varepsilon_1)$ est une base de F^2. Comme $M^2 - tM + dI_2 = 0$, on a $M(M\varepsilon_1) = -d\varepsilon_1 + tM\varepsilon_1$.

Autrement dit, si P est la matrice de $\mathscr{B}$ dans la base canonique, on a

$$P^{-1}MP = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}.$$

Ainsi, M est semblable à $C(t,d) = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$.

On a donc démontré le résultat suivant.

Pour compléter notre analyse, il faut déterminer les diverses classes de conjugaison à l'intérieur de chaque type.

Le cas des matrices de type I et II est facile, puisque deux matrices diagonalisables étant semblables si et seulement si elles ont même ensemble de valeurs propres.

Passons au type III. Deux matrices semblables ayant mêmes valeurs propres, pour tous $\lambda_1, \lambda_2 \in F$, si $T(\lambda_1)$ et $T(\lambda_2)$ sont semblables,alors $\lambda_1 = \lambda_2$. La réciproque est immédiate.

En ce qui concerne le type IV, comme deux matrices semblables ont même polynôme caractéristique, pour tous $t_1, t_2 \in F$ et tous $d_1, d_2 \in F^\times$, si les matrices $C(t_1, d_1)$ et $C(t_2, d_2)$ sont semblables, alors $(t_1, d_1) = (t_2, d_2)$. Encire une fois, la réciproque est immédiate.

On a donc démontré le théorème suivant.

Théorème 1.1. *Soit F un corps arbitraire. Alors, toute matrice de $\mathrm{GL}_2(F)$ est de type I,II,III ou IV, et deux matrices de types différents ne sont pas conjuguées.*

Si $M \in \mathrm{GL}_2(F)$, alors :

(1) *M est de type I si et seulement si elle est conjuguée à une matrice de la forme λI_2, avec $\lambda \in F^\times$.*

   De plus, pour tous $\lambda_1, \lambda_2 \in F^\times$, les matrices $\lambda_1 I_2$ et $\lambda_2 I_2$ sont conjuguées si et seulement si $\lambda_1 = \lambda_2$

(2) *M est de type II si et seulement si elle est conjuguée à une matrice diagonale $D(\lambda_1, \lambda_2) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, où $\lambda_1, \lambda_2 \in F^\times$ sont distincts.*

De plus, pour tous $\lambda_1, \lambda_1', \lambda_2, \lambda_2' \in F^\times$, les matrices $D(\lambda_1, \lambda_2)$ et $D(\lambda_1', \lambda_2')$ sont conjuguées si et seulement si $\{\lambda_1, \lambda_2\} = \{\lambda_1', \lambda_2'\}$

(3) *M est de type III si et seulement si elle est conjuguée à une matrice de la forme $T(\lambda) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, avec $\lambda \in F^\times$.*

De plus, pour tous $\lambda_1, \lambda_2 \in F^\times$, les matrices $T(\lambda_1)$ et $T(\lambda_2)$ sont conjuguées si et seulement si $\lambda_1 = \lambda_2$

(4) *M est de type IV si et seulement si elle est conjuguée à une matrice de la forme $C(t, d) = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$, avec $t \in F, d \in F^\times$ tels que $X^2 - tX + d$ est irréductible sur F.*

De plus, pour tous $(t_1, d_1), (t_2, d_2) \in F \times F^\times$ vérifiant les conditions requises, les matrices $C(t_1, d_2)$ et $C(t_2, d_2)$ sont conjuguées si et seulement si $(t_1, d_1) = (t_2, d_2)$.

Remarques 1.2.

(1) Si tout polynôme de degré 2 de $F[X]$ possède une racine dans F, il n'y a pas de matrices de type IV. C'est par exemple le cas si F est algébriquement clos.

(2) Il sera important pour a suite de comprendre à quelles conditions le polynôme $X^2 - tX + d$ est irréductible sur F.

Comme il est de degré 2, ce polynôme est irréductible si et seulement s'il n'est pas scindé sur F

Notons que s'il est scindé sur F, ses deux racines sont dans $F^\times$, puisque d est non nul.

Soit $\mathscr{P}_{1,2}(F^\times)$ l'ensemble des parties de $F^\times$ possédant un ou deux éléments.

Si $X = \{x_1, x_2\} \in \mathscr{P}_{1,2}(F^\times)$, on pose $c(X) = (x_1 + x_2, x_1 x_2) \in F \times F^\times$, où par convention $x_1 = x_2$ si X est un singleton. Notons que $c(X)$ ne dépend que de X, et pas de la numérotation de ses éléments. On obtient donc une application $c : \mathscr{P}_{1,2}(F^\times) \longrightarrow F \times F^\times$ bien définie.

Notons que l'application $c : \mathscr{P}_{1,2}(F^\times) \longrightarrow F \times F^\times$ est injective. En effet, si $X, Y \in \mathscr{P}_{1,2}(F^\times)$, l'égalité $c(X) = c(Y)$ revient à demander l'égalité des polynômes unitaires $T^2 - (x_1 + x_2)T + x_1 x_2$ et $T^2 - (y_1 + y_2)T + y_1 y_2$ (avec des notations évidentes), ce qui revient à demander l'égalité de leur ensemble de racines, à savoir X et Y respectivement.

L'ensemble des classes de conjugaison de matrices de type IV est alors en bijection avec $F \times F^\times \setminus \mathrm{Im}(c)$.

Nous allons finir ce paragraphe en déterminant le nombre de classe de conjugaisons de $\mathrm{GL}_2(F)$ lorsque F est un corps fini, ainsi que le cardinal de chaque classe. Pour cela, nous aurons besoin de déterminer le stabilisateur

d'une matrice sous l'action de conjugaison, c'est-à-dire sont centralisateur dans $\mathrm{GL}_2(F)$.

Si $M \in \mathrm{GL}_2(F)$, on pose

$$\mathscr{C}(M) = \{C \in \mathrm{GL}_2(F) \mid CM = MC\}.$$

Deux matrices conjuguées ayant des centralisateurs conjugués, il suffit de calculer $\mathscr{C}(M)$ lorsque M est une des matrices du théorème précédent.

Ceci est donné par la proposition suivante.

Proposition 1.3. *Soit $M \in \mathrm{GL}_2(F)$, et soit*

$$\mathscr{C}(M) = \{C \in \mathrm{GL}_2(F) \mid CM = MC\}.$$

Alors:

(1) *si $M = \lambda I_2$, avec $\lambda \in F^\times$, alors $\mathscr{C}(M) = \mathrm{GL}_2(F)$*

(2) *si $M = D(\lambda_1, \lambda_2)$, où $\lambda_1, \lambda_2 \in F^\times$ sont distincts, alors*

$$\mathscr{C}(M) = \{C \in \mathrm{GL}_2(F) \mid C \text{ diagonale}\}$$

(3) *si $M = T(\lambda)$, avec $\lambda \in F^\times$, alors*

$$\mathscr{C}(M) = \left\{ \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \mid r \in F^\times, s \in F \right\}$$

(4) *si $M = C(t, d)$, où $t \in F$ et $d \in F^\times$ sont tels que $X^2 - tX + d$ est irréductible sur F, on a*

$$\mathscr{C}(M) = \left\{ \begin{pmatrix} r & -du \\ u & r + tu \end{pmatrix} \mid r, u \in F, (r, u) \neq (0, 0) \right\}.$$

Démonstration. Soit $C = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathscr{C}(M)$.

Si $M = \lambda I_2$, avec $\lambda \in F^\times$, toute matrice C commute avec M, et on a

$$\mathscr{C}(\lambda I_2) = \mathrm{GL}_2(F).$$

Si $M = D(\lambda_1, \lambda_2)$, où $\lambda_1, \lambda_2 \in F^\times$ sont distincts, on a

$$CM = \begin{pmatrix} r\lambda_1 & s\lambda_2 \\ u\lambda_1 & c\lambda_2 \end{pmatrix} \text{ et } MC = \begin{pmatrix} r\lambda_1 & s\lambda_1 \\ u\lambda_2 & c\lambda_2 \end{pmatrix}.$$

Comme $\lambda_1 \neq \lambda_2$, on a $s = u = 0$, et C est diagonale. Inversement, toute matrice diagonale commute avec M, si bien que

$$\mathscr{C}(M) = \{C \in \mathrm{GL}_2(F) \mid C \text{ diagonale.}\}$$

Supposons que $M = T(\lambda)$, avec $\lambda \in F^\times$. On a

$$CM = \begin{pmatrix} r\lambda & r + s\lambda \\ u\lambda & u + v\lambda \end{pmatrix} \text{ et } MC = \begin{pmatrix} r\lambda + u & s\lambda + v \\ u\lambda & v\lambda \end{pmatrix}.$$

On obtient aisément $u = 0$ et $r = v$. Comme C est inversible, on a $r \in F^\times$.

On montre réciproquement qu'une matrice de la forme $\begin{pmatrix} r & s \\ 0 & r \end{pmatrix}$, avec $r \in F^\times$ et $s \in F$ commute avec M, et on a donc

$$C(M) = \{\begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \mid r \in F^\times, s \in F\}.$$

Supposons enfin que $M = C(t, d)$, où $t \in F$ et $d \in F^\times$ sont tels que $X^2 - tX + d$ est irréductible sur F.

On a

$$CM = \begin{pmatrix} s & -rd + st \\ v & -ud + vt \end{pmatrix} \text{ et } MC = \begin{pmatrix} -du & -dv \\ r + tu & s + tv \end{pmatrix}.$$

On a donc $s = -du, v = r + tu$ et $-rd + st = -dv$. Mais, les deux premières égalités entraînent la troisième. En effet, on a alors

$$-rd + st = -rd - dut = -d(r + tu) = -dv.$$

On a donc $C = \begin{pmatrix} r & -du \\ u & r + tu \end{pmatrix}$. Il faut encore s'assure de la non nullité du déterminant de C. On a $\det(C) = r^2 + tur + du^2$. On doit donc avoir en particulier $(r, u) \neq (0, 0)$. Si $u = 0$, alors nécessairement $r \neq 0$ et $\det(C) = r^2 \neq 0$. Si $u \neq 0$, on a $\det(C) = u^2 \chi_M(-\frac{r}{u}) \neq 0$, car χ_M est irréductible de degré 2 et n'a donc pas de racines dans F. Bref, $\det(C) \neq 0$ si et seulement si $(r, u) \neq (0, 0)$. L'inclusion manquante étant un simple calcul, ceci achève la démonstration. □

On suppose maintenant que F est un corps fini à q éléments. Rappelons que F est de caractéristique $p > 0$, où p est un nombre premier, et que le cardinal de F est alors une puissance de p.

Une matrice de $\mathrm{GL}_2(F)$ étant inversible si et seulement ses deux colonnes sont ne sont pas proportionnelles, on a $q^2 - 1$ choix pour la première colonne (une colonne ne peut être nulle) et $q^2 - q$ choix pour la seconde. Ainsi, on a

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

Si $M \in \mathrm{GL}_2(F)$, son stabilisateur sous l'action de conjugaison est $\mathscr{C}(M)$. Si $\mathrm{Conj}(M)$ est la classe de conjugaison de M, on a donc

$$|\mathrm{Conj}(M)| = \frac{|\mathrm{GL}_2(F)|}{|\mathscr{C}(M)|}.$$

On va maintenant dénombrer le nombre de classes de conjugaisons de chaque type ainsi que leur cardinal.

Nous allons nous appuyer sur le théorème 1.1, et sur le fait que les cardinaux des centralisateurs de deux matrices conjuguées sont égaux (ce qui est normal, puisqu'elles ont même classe de conjugaison).

Pour commencer, il y a $q-1$ classes de conjugaison de matrices de type I. Chaque classe de conjugaison contient un seul élément, puisque une matrice conjuguée à λI_2 lui est égale.

Il y a autant de classes de conjugaison de matrices de type II que d'éléments de parties à deux éléments de $F^\times$, à savoir $\dfrac{(q-1)(q-2)}{2}$. De plus, la proposition 1.3 montre que le centralisateur d'une telle matrice M possède $(q-1)^2$ éléments. La classe de conjugaison de M possède ainsi $q(q+1)$ éléments.

Un raisonnement identique montre qu'il y a $q-1$ classes de conjugaison de matrices de type III, et que le centraliseur possède $q(q-1)$ dans ce cas. La classe de conjugaison d'une telle matrice possède alors $(q-1)(q+1)$ éléments.

Enfin, il faut dénombrer le nombre de classes de conjugaison de matrices de type IV. D'après le théorème 1.1, et comme l'application $c : \mathscr{P}_{1,2}(F^\times) \longrightarrow F \times F^\times$ définie dans la remarque 1.2 (2) est injective, il y a $q(q-1) - |\mathscr{P}_{1,2}(F^\times)|$ telles classes de conjugaison, c'est-à-dire

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

Le cardinal du centralisateur est alors $q(q-1)$, et chaque classe contient donc $q(q-1)$ éléments.

Bref, on a le théorème suivant.

Théorème 1.4. *Soit F un corps à q éléments. Alors, toute matrice de $\mathrm{GL}_2(F)$ est de type I, II, III ou IV, et deux matrices de types différents ne sont pas conjuguées. De plus:*

(1) *il y a $q-1$ classes de conjugaison de matrices de type I, chacune possédant 1 élément*

(2) *il y a $\dfrac{(q-1)(q-2)}{2}$ classes de conjugaison de matrices de type II, chacune possédant $q(q+1)$ éléments*

(3) *il y a $q-1$ classes de conjugaison de matrices de type III, chacune possédant $(q-1)(q+1)$ éléments*

(4) *il y a $\dfrac{q(q-1)}{2}$ classes de conjugaison de matrices de type IV, chacune possédant $q(q-1)$ éléments.*

Au total, $\mathrm{GL}_2(F)$ possède $(q-1)(q+1)$ classes de conjugaison.

On finit en donnant un système complet de représentants des classes de conjugaison.

Théorème 1.5. *Soit F un corps à q éléments. On se fixe une numérotation arbitraire $\lambda_1, \dots, \lambda_{q-1}$ des éléments de $F^\times$. Alors, les matrices suivantes*

forment un système complet de représentants des classes de conjugaison de $\mathrm{GL}_2(F)$:

(1) *Type I: les* $q-1$ *matrices* $\lambda I_2,\ \lambda \in F^\times$, *dont les classes de conjugaison possèdent chacune* 1 *élément*

(2) *Type II: les* $\dfrac{(q-1)(q-2)}{2}$ *matrices* $\begin{pmatrix}\lambda_i & 0\\ 0 & \lambda_j\end{pmatrix},\ 1 \le i < j \le q-1$, *dont les classes de conjugaison possèdent chacune* $q(q+1)$ *éléments*

(3) *Type III: les* $q-1$ *matrices* $\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix},\ \lambda \in F^\times$, *dont les classes de conjugaison possèdent chacune* $(q-1)(q+1)$ *éléments*

(4) *Type IV: les* $\dfrac{q(q-1)}{2}$ *matrices* $\begin{pmatrix}0 & -d\\ 1 & t\end{pmatrix}$, *où* $t \in F$ *et* $d \in F^\times$ *sont tels que* $X^2 - tX + d$ *est irréductible sur* F, *dont les classes de conjugaison possèdent chacune* $q(q-1)$ *éléments.*

Remarque 1.6. Si l'on connait un générateur α du groupe cyclique $F^\times$, on peut bien sûr prendre $\lambda_i = \alpha^{i-1}$, pour tout $1 \le i \le q-1$.

2. Classes de conjugaison de $\mathrm{SL}_2(F)$

On suppose à nouveau que F un corps arbitraire. Commençons par définir quelques matrices de $\mathrm{SL}_2(F)$ qui nous intéresserons par la suite.

Deux matrices conjuguées dans $\mathrm{SL}_2(F)$ le sont dans $\mathrm{GL}_2(F)$. En particulier, un matrice de $\mathrm{SL}_2(F)$ appartient à un et un seul des quatre types de matrices définis dans $\mathrm{GL}_2(F)$.

Avant de continuer, remarquons que si M possède deux valeurs propres dans F (non nécessairement distinctes), leur produit est égal à $\det(M) = 1$.

En particulier, si M possède une unique valeur propre $\lambda \in F^\times$, simple ou double, alors $\det(M) = 1 = \lambda^2$, et par conséquent $\lambda = \pm 1$, et si M possède deux valeurs propres distinctes, eles sont nécessairement différentes de 1 et -1.

On peut donc affiner un peu la liste des types comme suit, en scindant les types I et III en deux sous-types chacun:

(1) Type I+: $\mu_M = X - 1$.

(2) Type I-: $\mu_M = X + 1$.

(3) Type II: $\mu_M = (X-\lambda)(X-\lambda^{-1})$, avec $\lambda \in F \setminus \{0, 1, -1\}$.

(4) Type III+: $\mu_M = (X-1)^2$

(5) Type III-: $\mu_M = (X+1)^2$

(6) Type IV: μ_M est irréductible sur F, de degré 2.

Si $\mathrm{car}(F) = 2$, on remarque les types $I+$ et $I-$ sont égaux, de même que les types $III+$ et $III-$. Par définition, chaque matrice possède un unique type, et deux matrices de types différents ne sont pas conjuguées.

Nous allons à nouveau analyser chaque cas, en faisant bien attention de conjuguer par des matrices de déterminant 1.

On commence par remarquer la chose suivante. Si $M, M' \in \mathrm{SL}_2(F)$, et si $Q \in \mathrm{GL}_2(F)$ vérifie $M = Q^{-1}M'Q$, alors $P = \begin{pmatrix} 1 & 0 \\ 0 & \det(Q)^{-1} \end{pmatrix} Q \in \mathrm{SL}_2(F)$ et on a $M = P^{-1}M''P$, avec

$$M'' = \begin{pmatrix} 1 & 0 \\ 0 & \det(Q)^{-1} \end{pmatrix} M' \begin{pmatrix} 1 & 0 \\ 0 & \det(Q) \end{pmatrix}.$$

Comme le produit de matrices diagonales est encore une matrice diagonale, cela montre qu'une matrice de type I ou II est semblable dans $\mathrm{SL}_2(F)$ à une matrice diagonale.

En particulier, une matrice de type I+ est semblable (et même égale) à I_2, une matrice de type I- est semblable (et même égale) à $-I_2$, tandis qu'une matrice de type II est semblable à une matrice de la forme

$$\Delta(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

avec $\lambda \in F \setminus \{0, 1, -1\}$.

Passons aux types III+ et III-. Si $M \in \mathrm{GL}_2(F)$ est de type III, elle est semblable dans $\mathrm{GL}_2(F)$ à une matrice de la forme $T(\lambda)$, où $\lambda \in F^\times$ est l'unique valeur propre de M. On rappelle que $\lambda = \pm 1$.

D'après les considérations précédentes, M est alors semblable dans $\mathrm{SL}_2(F)$ à

$$\begin{pmatrix} 1 & 0 \\ 0 & \delta^{-1} \end{pmatrix} T(\lambda) \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \lambda & \delta^{-1} \\ 0 & \lambda \end{pmatrix},$$

pour un certain $\delta \in F^\times$. En tenant compte du fait que $\lambda = \pm 1$, en changeant un peu les notations, on voit qu'une matrice de type III+ est semblable à une matrice de la forme $\Theta(\alpha)$, et une matrice de type III- est semblable à une matrice de la forme $-\Theta(\alpha)$, avec $\alpha \in F^\times$, où on a posé

$$\Theta(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

On verra plus loin que, contrairement au cas de $\mathrm{GL}_2(F)$, on ne peut pas s'arranger pour prendre $\alpha = 1$.

Il reste à étudier le cas des matrices de type IV. Une telle matrice M est semblable dans $\mathrm{GL}_2(F)$ à une matrice de la forme $C(t, d)$, où $t \in F, d \in F^\times$ sont tels que $X^2 - tX + d$ soit irréductible sur F. Comme la conjugaison

préserve le déterminant, on a $d = 1$. En raisonnant comme précédemment, on voit que M est semblable dans $\mathrm{SL}_2(F)$ à une matrice de la forme

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

où $\delta \in F^\times$ et $t \in F$ est tel que $X^2 - tX + 1$ soit irréductible sur F.

On note cette dernière matrice $\Gamma(t, \delta)$.

Encore une fois, il faut maintenant distinguer les classes de conjugaison au sein de chaque type de matrices. Cela est beaucoup moins immédiat que pour le cas de $\mathrm{GL}_2(F)$, et va dépendre de F, contrairement au cas précédent.

Pour les matrices de type I+ et I-, c'est facile, puisque dans chaque cas, deux matrices conjuguées sont égales.

Pour les matrices de type II, pour tous $\lambda_1, \lambda_2 \in F \setminus \{0, 1, -1\}$, on remarque que si $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^{-1} \end{pmatrix}$ et $\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^{-1} \end{pmatrix}$ sont conjuguées dans $\mathrm{SL}_2(F)$, elles ont même ensemble de valeurs propres, et on a donc $\{\lambda_1, \lambda_1^{-1}\} = \{\lambda_2, \lambda_2^{-1}\}$, soit encore $\lambda_2 = \lambda_1$ ou $\lambda_2 = \lambda_1^{-1}$. La réciproque découle alors de l'égalité

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix},$$

pour tout $\lambda \in F^\times$.

Passons aux matrices de type III+ et III-. On commence par remarquer que pour tout $\alpha \in F^\times$, $\Theta(\alpha)$ et $-\Theta(\alpha)$ ne sont pas conjuguées (puisqu'elles n'ont pas les mêmes valeurs propres), sauf si F est de caractéristique 2. De plus, $\Theta(\alpha_1)$ et $\Theta(\alpha_2)$ sont conjuguées si et seulement leurs opposées le sont.

Il faut donc déterminer sous quelles conditions deux matrices $\Theta(\alpha_1)$ et $\Theta(\alpha_2)$ sont conjuguées.

Soient $\alpha_1, \alpha_2 \in F^\times$, et soit $C = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(F)$ telle que $C\Theta(\alpha_1)C^{-1} = \Theta(\alpha_2)$. On a donc $C\Theta(\alpha_1) = \Theta(\alpha_2)C$.

Or, on a

$$C\Theta(\alpha_1) = \begin{pmatrix} r & r\alpha_1 + s \\ u & u\alpha_1 + v \end{pmatrix} \text{ et } \Theta(\alpha_2)C = \begin{pmatrix} r + \alpha_2 u & s + \alpha_2 v \\ u & v \end{pmatrix}.$$

Puisque $\alpha_2 = 0$, on obtient aisément $u = 0$, ainsi que $v = \alpha_2^{-1}\alpha_1 r$. Comme $\det(C) = 1$, on en déduit $\alpha_2 = \alpha_1 r^2$. Notons que r est non nul puisqu C est inversible. Inversement, si $\alpha_2 = \alpha_1 r^2$, avec $r \in F^\times$, on vérifie que

$$\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \Delta(\alpha_1) \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}^{-1} = \Delta(\alpha_2).$$

Il rest à régler le cas des matrices de type IV. Soient $t_1, t_2 \in F$ tels que les polynômes $X^2 - t_1 X + 1$ et $X^2 - t_2 X + 1$ soient irréductibles sur F, et soient

$\delta_1, \delta_2 \in F^\times$. Si $\Gamma(t_1, \delta_1)$ et $\Gamma(t_2, \delta_2)$ sont conjuguées dans $\mathrm{SL}_2(F)$, elles ont même trace et donc $t_1 t = t_2$. On note t cette valeur commune.

Soit $C = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(F)$ telle que $C\Gamma(t, \delta_1)C^{-1} = \Theta(t, \delta_2)$. On a donc $C\Gamma(t, \delta_1) = \Theta(t, \Gamma_2)C$.

Or, on a

$$C\Gamma(t, \delta_1) = \begin{pmatrix} s\delta_1^{-1} & -r\delta_1 + st \\ v\delta_1^{-1} & -u\delta_1 + vt \end{pmatrix} \text{ et } \Gamma(t, \delta_2)C = \begin{pmatrix} -\delta_2 u & -\delta_2 v \\ \delta_2^{-1} r + tu & \delta_2^{-1} s + tv \end{pmatrix}.$$

On vérifie que cette égalité équivaut aux deux conditions $s\delta_1^{-1}u = -\delta_2 u$ et $-r\delta_1 + st = -\delta_2 v$. On a ainsi $s = -\delta_1\delta_2 u$, puis $-r\delta_1 - \delta_1\delta_2 ut = -\delta_2 v$, soit $v = \delta_2^{-1}\delta_1(r + \delta_2 ut)$. On a alors

$$\det(C) = \delta_2^{-1}\delta_1(r^2 + \delta_2 rut) + \delta_1\delta_2 u^2 = \delta_2^{-1}\delta_1(r^2 + tr(u\delta_2) + (u\delta_2)^2) = 1,$$

soit encore $\delta_2 = \delta_1(r^2 + tr(u\delta_2) + (u\delta_2)^2)$. Notons que $(r, u) \neq (0, 0)$, puisque δ_1 et δ_2 sont non nuls. Inversement, supposons qu'il existe $x, y \in F$, non tous deux nuls, tels que $\delta_2 = \delta_1(x^2 + txy + y^2)$, on vérifie que l'on a

$$\begin{pmatrix} x & -\delta_1 y \\ \delta_2^{-1} y & \delta_2^{-1}\delta_1(x + ty) \end{pmatrix} \Gamma(t, \delta_1) \begin{pmatrix} x & -\delta_1 y \\ \delta_2^{-1} y & \delta_2^{-1}\delta_1(x + ty) \end{pmatrix}^{-1} = \Gamma(t, \delta_2).$$

Notons que la matrice par laquelle on conjugue est bien de déterminant 1, vu l'hypothèse sur δ_1 et δ_2. Afin d'interpréter au mieux ce résultat, on va introduire quelques notations.

Soit $L_t = F[X]/(X^2 - tX + 1)$. Comme $X^2 - tX + 1$ est irréductible sur F, c'est un corps. De plus, c'est un F-espace vectoriel pour la loi externe

$$\begin{aligned} F \times L_t &\longrightarrow L_t \\ (\lambda, \overline{f}) &\longmapsto \lambda \cdot \overline{f} = \overline{\lambda f}. \end{aligned}$$

de dimension 2, de base $(\overline{1}, \overline{X})$, où $\omega = \overline{X}$.

Cela provient du fait que tout élement du quotient est représenté par un unique polynôme de degré ≤ 2. En particulier, le morphisme $\begin{aligned} F &\longrightarrow L_t \\ \lambda &\longmapsto \lambda \cdot \overline{1} = \overline{\lambda} \end{aligned}$ étant injectif, on peut identifier canoniquement F à son image.

Avec ce léger abus de notation, si l'on pose $\omega = \overline{X}$, tout élément de L_t s'écrit de manière unique sous la forme $x + y \cdot \omega, x, y, \in F$.

Par définition de ω, on a $\omega^2 - t\omega + 1 = 0$, si bien que les opérations dans L_t se récrivent

$$(x + y \cdot \omega) + (x' + y' \cdot \omega) = (x + x') + (y + y') \cdot \omega$$

et

$$(x + y \cdot \omega)(x' + y' \cdot \omega) = (xx' - yy') + (xy' + x'y - tyy') \cdot \omega,$$

pour tous $x, x', y, y' \in F$.

Si $\alpha \in L_t$, on définit la *norme* de α, notée $N_{L_t/F}(\alpha)$, comme le déterminant de l'endomorphisme

$$\ell_\alpha : \begin{array}{ccc} L_t & \longrightarrow & L_t \\ \beta & \longmapsto & \alpha\beta. \end{array}$$

Notons que si $\alpha \in L_t^\times$, l'endomorphisme ℓ_α est bijective, d'inverse $\ell_{\alpha^{-1}}$, et donc $N_{L_t/F}(\alpha) \in F^\times$ dans ce cas.

De plus, pour tous $\alpha_1, \alpha_2 \in L_t$, on a

$$N_{L_t/F}(\alpha_1\alpha_2) = \det(\ell_{\alpha_1\alpha_2}) = \det(\ell_{\alpha_1} \circ \ell_{\alpha_2}) = \det(\ell_{\alpha_1}) \det(\ell_{\alpha_2}) = N_{L_t/F}(\alpha_1) N_{L_t/F}(\alpha_2).$$

En particulier, l'aplication $N_{L_t/F} : L^\times \longrightarrow F^\times$ est un morphisme de groupes.

Enfin, si $\alpha = x + y \cdot \omega$, on a

$$\alpha\omega = -y + (x + ty) \cdot \omega.$$

La matrice de ℓ_α dans la base $(1, \omega)$ est alors donnée par

$$\begin{pmatrix} x & -y \\ y & x + ty \end{pmatrix}.$$

On a donc $N_{L_t/F}(\alpha) = x^2 + txy + y^2$.

Les résultats précédents se réinterprètent maintenant en disant que pour tout $t \in F$ tel que $X^2 - tX + 1$ est irréductible sur F et tous $\delta_1, \delta_2 \in F^\times$, les matrices $C(t, \delta_1) = et = C(t, \delta_2)$ sont conjuguées si et seulement si $\overline{\delta}_1 = \overline{\delta}_2 \in F^\times / N_{L_t/F}(L_t^\times)$.

On a donc démontré le théorème suivant.

Théorème 2.1. *Soit F un corps arbitraire.*

Si $\mathrm{car}(F) \neq 2$, *toute matrice de* $\mathrm{SL}_2(F)$ *est de type $I+, I-, II, III+, III-$ ou IV.*

Si $\mathrm{car}(F) = 2$, *toute matrice de* $\mathrm{SL}_2(F)$ *est de type $I+, II, III+$ ou IV.*

Dans les deux cas, deux matrices de types différents ne sont pas conjuguées.

Soit $M \in \mathrm{SL}_2(F)$. Alors,

(1) *I_2 est l'unique matrice de type $I+$*

(2) *$-I_2$ est l'unique matrice de type $I-$*

(3) *M est de type II si et seulement si elle est conjuguée à une matrice de la forme $\Delta(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, avec $\lambda \in F \setminus \{0, 1, -1\}$.*

De plus, pour tous $\lambda_1, \lambda_2 \in F \setminus \{0, 1, -1\}$, les matrice $\Delta(\lambda_1)$ et $\Delta(\lambda_2)$ sont semblables si et seulement si $\{\lambda_1, \lambda_1^{-1}\} = \{\lambda_2, \lambda_2^{-1}\}$.

(4) *M est de type $III+$ si et seulement si elle est conjuguée à une matrice de la forme $\Theta(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, avec $\alpha \in F^\times$.*

De plus, pour tous $\alpha_1, \alpha_2 \in F^\times$, les matrices $\Theta(\alpha_1)$ et $\Theta(\alpha_2)$ sont conjuguées si et seulement si $\overline{\alpha}_1 = \overline{\alpha}_2 \in F^\times/F^{\times 2}$.

(5) *M est de type III- si et seulement si elle est conjuguée à une matrice de la forme $-\Theta(\alpha)$, avec $\alpha \in F^\times$.*

De plus, pour tous $\alpha_1, \alpha_2 \in F^\times$, les matrices $-\Theta(\alpha_1)$ et $-\Theta(\alpha_2)$ sont conjuguées si et seulement si $\overline{\alpha}_1 = \overline{\alpha}_2 \in F^\times/F^{\times 2}$.

(6) *M est de type IV si et seulement si elle est conjuguée à une matrice de la forme $\Gamma(t,\delta) = \begin{pmatrix} 0 & -\delta \\ \delta^{-1} & t \end{pmatrix}$, où $t \in F$ est tel que $X^2 - tX + 1$ soit irréductible sur F et $\delta \in F^\times$.*

De plus, pour tous $(t_1, \delta_1), (t_2, \delta_2) \in F \times F^\times$, avec t_1, t_2 vérifiant les conditions requises, les matrices $C(t_1, \delta_1)$ et $C(t_2, \delta_2)$ sont conjuguées si et seulement s'il existe $t \in F$ tel que $t_1 = t_2 = t$ et $\overline{\delta}_1 = \overline{\delta}_2 \in F^\times/N_{L_t/F}(L_t^\times)$.

Remarques 2.2.

(1) Si tout polynôme de degré 2 de $F[X]$ possède une racine, il n'y a pas de matrice de type IV. De plus, tout élément de F est alors un carré et toute matrice de type III+ (resp. III-) est conjuguée) à $\Theta(1)$ (resp. $-\Theta(1)$).

(2) En faisant un raisonnement similaire à celui fait pour le cas de $\mathrm{GL}_2(F)$, on constate que le polynôme $X^2 - tX + 1$ est irréductible sur F si et seulement t n'est pas dans l'image de l'application injective

$$\begin{aligned} \gamma : \Pi_{1,2}(F) &\longrightarrow F \\ X = \{x, x^{-1}\} &\longmapsto x + x^{-1}, \end{aligned}$$

où $\Pi_{1,2}(F)$ est l'ensemble des parties de $F^\times$ de la forme $\{x, x^{-1}\}$.

Comme pour le cas de $\mathrm{GL}_2(F)$, nous allons nous intéresser au cas des corps finis. Pour cela, nous aurons besoin de calculer le centraliseur de $M \in \mathrm{SL}_2(F)$ dans $\mathrm{SL}_2(F)$. On le note $\mathscr{C}_1(M)$.

On a la proposition suivante.

Proposition 2.3. *Soit $M \in \mathrm{SL}_2(F)$, et soit*

$$\mathscr{C}_1(M) = \{C \in \mathrm{SL}_2(F) \mid CM = MC\}.$$

Alors:

(1) *si $M = \pm I_2$, alors $\mathscr{C}_1(M) = \mathrm{SL}_2(F)$*
(2) *si $M = \Delta(X)$, où $X = \{\lambda, \lambda^{-1}\}$, avec $\lambda \in F \setminus \{0, 1, -1\}$, alors*

$$\mathscr{C}_1(M) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in F^\times \right\}$$

(3) *si $M = \pm\Theta(\alpha)$, avec $\alpha \in F^\times$, alors*

$$\mathscr{C}_1(M) = \left\{ \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \mid r \in \{1, -1\}, s \in F \right\}$$

(4) *si* $M = \Gamma(t, \delta)$, *où* $t \in F$ *est tel que* $X^2 - tX + 1$ *est irréductible sur* F *et* $\delta \in F^\times$, *on a*

$$\mathscr{C}_1(M) = \left\{ \begin{pmatrix} x & -\delta y \\ \delta^{-1} y & x + ty \end{pmatrix} \mid \alpha = x + y \cdot \omega \in L_t^\times, N_{L_t/F}(\alpha) = 1 \right\}.$$

Démonstration. On va s'appuyer sur l'égalité évidente suivante: pour toute matrice $M \in \mathrm{SL}_2(F)$, on a $\mathscr{C}_1(M) = \mathscr{C}(M) \cap \mathrm{SL}_2(F)$.

Les points (1) et (2) découlent alors immédiatement de la proposition 1.3.

En ce qui concerne le point (3), on commence par remarquer que $C \in \mathrm{SL}_2(F)$ commute avec M si et seulement si elle commute avec $-M$, si bien que $\mathscr{C}_1(-M) = \mathscr{C}_1(M)$. On peut donc se limiter au cas $M = \Theta(\alpha)$.

De plus, on a $\Theta(\alpha) = \alpha^{-1} T(\alpha^{-1})$, si bien que l'on a les égalités

$$\mathscr{C}_1(\Theta(\alpha)) = \mathscr{C}_1(T(\alpha^{-1})) = \mathscr{C}(T(\alpha^{-1})) \cap \mathrm{SL}_2(F).$$

On applique alors la proposition 1.3 pour conclure.

Finalement, supposons que $M = \Gamma(t, \delta)$, avec $\delta \in F^\times$ et $t \in F$ tel que $X^2 - tX + 1$ soit irréductible sur F. Remarquons que l'on a l'égalité

$$M = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}^{-1} C(t, 1) \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}.$$

Par conséquent, on a aussi

$$\mathscr{C}(M) = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}^{-1} \mathscr{C}(C(t, 1)) \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix},$$

et puisque deux matrices conjuguées ont même déterminant, on en déduit

$$\mathscr{C}_1(M) = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}^{-1} \mathscr{C}_1(C(t, 1)) \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}.$$

La proposition 1.3 et un petit calcul matriciel donne alors le résultat souhaité. □

On suppose maintenant que F est un corps fini. Avant de pouvoir dénombrer le nombre de classes de conjugaison de chaque type et leurs cardinaux, on a besoin d'un résultat intermédiaire.

Lemme 2.4. *Soit* F *un corps fini à* q *éléments.*

(1) *Si* $\mathrm{car}(F) = 2$, *le groupe* $F^\times / F^{\times 2}$ *est trivial.*

(2) *Si* $\mathrm{car}[F) \neq 2$, *le groupe* $F^\times / F^{\times 2}$ *a deux éléments.*

(3) *Soit* $t \in F$ *tel que* $X^2 - tX + 1$ *soit irréductible sur* F. *Alors, l'application* $N_{L_t/F} : L_t^\times \longrightarrow F^\times$ *est surjective, et* $\ker(N_t)$ *possède* $q + 1$ *éléments.*

Démonstration. Notons que le morphisme de groupes

$$F^\times \longrightarrow F^{\times 2}$$
$$x \longmapsto x^2$$

est surjective, de noyau $\{1,-1\}$. Le théorème de factorisation donne alors l'égalité

$$\frac{|F^\times|}{|\{1,-1\}|} = |F^{\times 2}|,$$

d'où $|F^\times/F^{\times 2}| = |\{1,-1\}|$. Notons que $\{1,-1\}$ possède un élément si $\mathrm{car}(F) = 2$, et deux éléments si $\mathrm{car}(F) \neq 2$. Cela démontre les deux premiers points.

On obtient aussi le fait que $N_{L_t/F}$ est surjective si $\mathrm{car}(F) = 2$. En effet, si $x \in F^\times$, il existe $y \in F^\times$ tel que $x = y^2$ d'après (1), et on a alors $N_{L_t/F}(y) = y^2 = x$.

Supposons maintenant que $\mathrm{car}(F) \neq 2$. Pour tous $x, y \in F$, on a

$$N_{L_t/F}(x + y\cdot\omega) = x^2 + txy + y^2 = (x + \frac{ty}{2})^2 + (1 - \frac{t^2}{4})y^2.$$

Remarque que $a = 1 - \dfrac{t^2}{4}$ est non nul, car sinon, on aurait $t = \pm 2$ et $X^2 - tX + 1 = (X \pm 1)^2$ ne serait pas irréductible.

Soit $z \in F^\times$. L'ensemble $\{z - r^2 \mid r \in F\}$ est en bijection avec $\{r^2 \mid r \in F\} = F^{\times 2} \cup \{0\}$, et possède donc $\dfrac{q-1}{2} + 1 = \dfrac{q+1}{2}$ éléments, d'après le point (2).

D'autre part, puisque a est non nul, l'ensemble $\{as^2 \mid s \in F\}$ possède également $\dfrac{q+1}{2}$. Ces deux ensembles ne peuvent donc être disjoints, car la somme de leurs cardinaux vaut $q+1$ et F possède q éléments. Il existe donc $r, s \in F$ tels que $r^2 + as^2 = z$.

Si l'on pose $x = r - \dfrac{ts}{2}$ et $y = s$, on obtient $N_{L_t/F}(x + y\cdot\omega) = z$. Notons que x et y ne peuvent être tous deux nuls, car $z \neq 0$. Ceci prouve la surjectivité voulue dans ce cas.

Indépendemment de la caractéristique de F, le théorème de factorisation, appliqué au morphisme surjectif $N_{L_t/F} : L_t^\times \longrightarrow F^\times$ montre que l'on a

$$\frac{|L_t^\times|}{|\ker(N_{L_t/F})|} = |F^\times|.$$

Comme L est de dimension 2 sur F, on a $|L| = q^2$, et on obtient alors $|\ker(N_{L_t/F})| = \dfrac{q^2-1}{q-1} = q+1$. □

Nous somme maintenant en mesure de compter le nombre de classes de conjugaison et leurs nombres d'éléments.

Le théorème de factorisation, appliqué au morphisme surjectif $\det : \mathrm{GL}_2(F) \longrightarrow F^\times$, donne

$$\frac{|\mathrm{GL}_2(F)|}{|\mathrm{SL}_2(F)|} = q - 1,$$

d'où $|\mathrm{SL}_2(F)| = q(q-1)(q+1)$.

Si $M \in \mathrm{SL}_2(F)$, son stabilisateur sous l'action de conjugaison est $\mathscr{C}_1(M)$. Si $\mathrm{Conj}_1(M)$ est la classe de conjugaison de M, on a donc

$$|\mathrm{Conj}_1(M)| = \frac{|\mathrm{SL}_2(F)|}{|\mathscr{C}_1(M)|}.$$

Nous nous appuyerons cette fois sur le théorème 2.1, et sur le fait que les cardinaux des centralisateurs de deux matrices conjuguées sont égaux.

Pour le type I+ et I-, il y a une seule classe de conjugaison, contenant un seul élément.

De plus, il y a $|\Pi_2(F)|$ classes de conjugaison de matrices de type II, où $\Pi_2(F)$ est l'ensemble des parties de $F \setminus \{0, 1, -1\}$ à deux éléments de la forme $\{x, x^{-1}\}$. Si $x, y \in F \setminus \{0, 1, -1\}$, les ensembles $\{x, x^{-1}\}$ et $\{ y, y^{-1}\}$ sont égaux si seulement si $y = x$ ou x^{-1}. Comme x et x^{-1} sont distincts, on a

$$|\Pi_2(F)| = \frac{|F \setminus \{0, 1, -1\}|}{2} = \begin{cases} \dfrac{q-3}{2} & \text{si } \mathrm{car}(F) \neq 2 \\ \dfrac{q-2}{2} & \text{si } \mathrm{car}(F) = 2 \end{cases}$$

D'autre part, la proposition 2.3 montre que si M est de type II, $|\mathscr{C}_1(M)| = q - 1$. Une classe de conjugaison possède donc $q(q + 1)$ éléments.

En ce qui concerne les matrices de type III+, le lemme précédent et le théorème 2.1 montrent qu'il y a 2 classes de conjugaison si $\mathrm{car}(F) \neq 2$, et 1 classe si $\mathrm{car}(F) = 2$.

La proposition 2.3 montre alors que si M est de type III+, $\mathscr{C}_1(M)$ possède $2q$ éléments si $\mathrm{car}(F) \neq 2$, et q éléments si $\mathrm{car}(F) = 2$. Par conséquent, la classe de conjugaison de M possède $\dfrac{(q-1)(q+1)}{2}$ éléments si $\mathrm{car}(F) \neq 2$, et $(q - 1)(q + 1)$ éléments si $\mathrm{car}(F) = 2$.

Les résultats sont identiques pour les classes de conjugaison de type III-.

Le théorème 2.1 et le lemme précédent montrent qu'il y a $|F \setminus \mathrm{Im}(\gamma)|$ classes de conjugaison de matrices de type IV, où $\gamma : \Pi_{1,2}(F) \longrightarrow F$ est l'application injective définie dans la remarque 2.2 (2).Ici, $\Pi_{1,2}(F)$ désigne l'ensemble des parties de $F^\times$ de la forme $\{x, x^{-1}\}$. Comme γ est injective, ce nombre est égal à $|F \setminus \Pi_{1,2}(F)|$.

Notons que $\Pi_{1,2}(F) = \{1, -1\} \bigsqcup \Pi_2(F)$, où $\bigsqcup$ désigne l'union disjointe. D'après un calcul précédent, on en déduit que

$$|F \setminus \Pi_{1,2}(F)| = \begin{cases} \dfrac{q-1}{2} & \text{si } \mathrm{car}(F) \neq 2 \\ \dfrac{q}{2} & \text{si } \mathrm{car}(F) = 2 \end{cases}$$

De plus, le théorème 2.1 et le lemme précédent montrent que si M est de type IV, $|\mathscr{C}_1(M)| = q+1$. Ainsi, sa classe de conjugaison comporte $q(q-1)$ éléments.

On a donc le résultat suivant.

Théorème 2.5. *Soit F un corps à q éléments.*

Si $\mathrm{car}(F) \neq 2$, *toute matrice de* $\mathrm{SL}_2(F)$ *est de type* $I+, I-, II, III+, III-$ *ou* IV, *et deux matrices de types différents ne sont pas conjuguées. De plus:*

(1) *il y a* 1 *classe de conjugaison de matrices de type* $I+$, *possédant* 1 *élément*
(2) *il y a* 1 *classe de conjugaison de matrices de type I-, possédant* 1 *élément*
(3) *il y a* $\dfrac{q-3}{2}$ *classes de conjugaison de matrices de type II, chacune possédant* $q(q+1)$ *éléments*
(4) *il y a* 2 *classes de conjugaison de matrices de type III+, chacune possédant* $\dfrac{(q-1)(q+1)}{2}$ *éléments*
(5) *il y a* 2 *classes de conjugaison de matrices de type III-, chacune possédant* $\dfrac{(q-1)(q+1)}{2}$ *éléments*
(6) *il y a* $\dfrac{q-1}{2}$ *classes de conjugaison de matrices de type IV, chacune possédant* $q(q-1)$ *éléments.*

Au total, $\mathrm{SL}_2(F)$ *possède* $q+4$ *classes de conjugaison dans ce cas.*

Si $\mathrm{car}(F) = 2$, *toute matrice de* $\mathrm{SL}_2(F)$ *est de type* $I+, II, III+$ *ou* IV, *et deux matrices de types différents ne sont pas conjuguées. De plus:*

(1) *il y a* 1 *classe de conjugaison de matrices de type* $I+$, *possédant* 1 *élément*
(2) *il y a* $\dfrac{q-2}{2}$ *classes de conjugaison de matrices de type II, chacune possédant* $q(q+1)$ *éléments*
(3) *il y a* 1 *classe de conjugaison de matrices de type III+, possédant* $(q-1)(q+1)$ *éléments*
(4) *il y a* $\dfrac{q}{2}$ *classes de conjugaison de matrices de type IV, chacune possédant* $q(q-1)$ *éléments.*

Au total, $\mathrm{SL}_2(F)$ *possède* $q+1$ *classes de conjugaison dans ce cas.*

Grâce au lemme 2.4 et tous les résultats précédents, on peut également donner un système complet de classes de conjugaison de $\mathrm{SL}_2(F)$, lorsque F est un corps fini.

Théorème 2.6. *Soit F un corps fini à q éléments. Soit E une partie de F telle que*

$$F = \{0, 1, -1\} \sqcup \bigsqcup_{x \in E} \{x, x^{-1}\}.$$

Si $\mathrm{car}(F) \neq 2$, *on fixe $\varepsilon \in F^\times \setminus F^{\times 2}$. Alors, les matrices suivantes forment un système complet de représentants de classes de conjugaison de* $\mathrm{SL}_2(F)$*:*

(1) *Type I+: I_2. Sa classe de conjugaison possède* 1 *élément.*

(2) *Type I-: $-I_2$. Sa classe de conjugaison possède* 1 *élément.*

(3) *Type II: les* $\dfrac{q-3}{2}$ *matrices* $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$, $x \in E$. *La classe de conjugaison de chacune de ces matrices possède $q(q+1)$ éléments.*

(4) *Type III+: les* 2 *matrices* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}$. *La classe de conjugaison de chacune de ces matrices possède* $\dfrac{(q-1)(q+1)}{2}$ *éléments.*

(5) *Type III-: les* 2 *matrices* $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & -\varepsilon \\ 0 & -1 \end{pmatrix}$. *La classe de conjugaison de chacune de ces matrices possède* $\dfrac{(q-1)(q+1)}{2}$ *éléments.*

(6) *Type IV: les* $\dfrac{q-1}{2}$ *matrices* $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$, *où $t \in F \setminus \mathrm{Im}(\gamma)$. La classe de conjugaison de chacune de ces matrices possède $q(q-1)$ éléments.*

Si $\mathrm{car}(F) = 2$, *les matrices suivantes forment un système complet de représentants de classes de conjugaison de* $\mathrm{SL}_2(F)$*:*

(1) *Type I+: I_2. Sa classe de conjugaison possède* 1 *élément.*

(2) *Type II: les* $\dfrac{q-2}{2}$ *matrices* $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$, $x \in E$. *La classe de conjugaison de chacune de ces matrices possède $q(q+1)$ éléments.*

(3) *Type III+:* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. *Sa classe de conjugaison possède $(q-1)(q+1)$ éléments.*

(4) *Type IV: les* $\dfrac{q}{2}$ *matrices* $\begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix}$, *où $t \in F \setminus \mathrm{Im}(\gamma)$. La classe de conjugaison de chacune de ces matrices possède $q(q-1)$ éléments.*

3. Classes de conjugaison de $\mathrm{PSL}_2(F)$

On suppose à nouveau que F un corps quelconque. Rappelons que $\mathrm{PSL}(F)$ est le groupe quotient $\mathrm{SL}_2(F)/\{\pm I_2\}$.

En particulier, si $\mathrm{car}(F) = 2$, on a $\mathrm{PSL}_2(F) = \mathrm{SL}_2(F)$ et le travail a déjà été fait dans le paragraphe précédent.

On suppose dorénavant, sauf mention du contraire, que $\mathrm{car}(F) \neq 2$.

Si $M \in \mathrm{SL}_2(F)$, on note $\overline{M}$ sa classe dans $\mathrm{PSL}_2(F)$. Notons que si $M \in \mathrm{SL}_2(F)$, on a $\mu_{-M} = \mu_M(-X)$.

Notons que $\mu_M(-X)$ a même degré et même nombre de racines que μ_M. En particulier, l'opération $M \rightsquigarrow -M$ conserve les types II et IV, et échange les types I+ et I-, resp. III+ et III-.

Par conséquent, un élément de $\mathrm{PSL}_2(F)$ peut toujours être représenté par une matrice de type $I+, II, III+$ ou IV.

On dira qu'un élément de $\mathrm{PSL}_2(F)$ est de type I+,II,III+ ou IV s'il est représenté par une matrice de $\mathrm{SL}_2(F)$ de ce même type.

Notons que, pour tous $M_1, M_2 \in \mathrm{SL}_2(F)$, $\overline{M}_1$ et $\overline{M}_2$ sont conjugués dans $\mathrm{PSL}_2(F)$ si et seulement si M_1 et M_2 sont conjuguées dans $\mathrm{SL}_2(F)$ ou M_1 et $-M_2$ sont conjuguées dans $\mathrm{SL}_2(F)$.

D'après les considérations précédentes, si M_1 et M_2 ont des types différents parmi les types I+,II,III+ et IV, il en est de même pour M_1 et $-M_2$. En effet, le fait que M_1 et M_2 sont de types différents revient à dire que leurs polynômes minimaux n'ont pas le même nombre de racines dans F, ce qui est alors aussi vrai pour les polynômes minimaux de M_1 et $-M_2$.

Grâce au théorème 2.1, on obtient que toute classe de $\mathrm{PSL}_2(F)$ est de type I+,II,III+ ou IV, et deux classes de types différents ne sont pas conjuguées.

De plus, si $\overline{M} \in \mathrm{PSL}_2(F)$, alors:

(1) $\overline{I}_2$ est l'unique élément de type I

(2) $\overline{M}$ est de type II si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Delta(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, avec $\lambda \in F \setminus \{0, 1, -1\}$.

(3) $\overline{M}$ est de type III+ si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Theta(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, avec $\alpha \in F^\times$

(4) $\overline{M}$ est de type IV si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Gamma(t, \delta) = \begin{pmatrix} 0 & -\delta \\ \delta^{-1} & t \end{pmatrix}$, où $\delta \in F^\times$ et $t \in F$ est tel que $X^2 - tX + 1$ soit irréductible sur F.

Il faut maintenant déterminer les classes de conjugaison pour chaque type. Encore une fois, il n'y a qu'une classe de conjugaison de type I+, à savoir celle de $\overline{I_2}$.

Passons au type II. Soient $\lambda_1, \lambda_2 \in F^\times\{0, 1, -1\}$, et posons $M_i = \begin{pmatrix} \lambda_i & 0 \\ 0 & \lambda_i^{-1} \end{pmatrix}$ pour $i = 1, 2$.

Alors M_1 est conjuguée à M_2 ou $-M_2$ si et seulement si $\{\lambda_1, \lambda_1^{-1}\} = \{\lambda_2, \lambda_2^{-1}\}$ ou $\{-\lambda_2, -\lambda_2^{-1}\}$, ce qui revient à dire que $\lambda_2 \in \{\lambda_1, -\lambda_1, \lambda - 1^{-1}, -\lambda_1^{-1}\}$. On voit facilement que c'est équivalent à demander l'égalité

$$\{\lambda_1, -\lambda_1, \lambda_1^{-1}, -\lambda_1^{-1}\} = \{\lambda_2, -\lambda_2, \lambda_2^{-1}, -\lambda_2^{-1}\}$$

Passons au type III+. Si $M_1, M_2 \in \mathrm{SL}_2(F)$ sont de type III+, alors M_2 est de type III-. Par conséquent, M_1 et $-M_2$ ne peuvent être conjuguées. Il s'ensuit que $\overline{M}_1$ et $\overline{M}_2$ sont conjuguées dans $\mathrm{PSL}_2(F)$ si et seulement si M_1 et M_2 sont conjuguées dans $\mathrm{SL}_2(F)$.

Il reste à examiner le type IV. Soient $M_1 = \Gamma(t_1, \delta_1)$ et $M_2 = \Gamma(t_2, \delta_2)$ deux matrices de $\mathrm{SL}_2(F)$ de type IV. Remarquons que $-M_2 = \Gamma(-t_2, -\delta_2)$. Les classes $\overline{M}_1$ et $\overline{M}_2$ sont alors conjuguées si et seulement s'il existe $t \in F \setminus \{Im(\gamma)\}$ tel qu'au moins une des deux conditions suivantes est vérifiée:

(1) $t_1 = t, t_2 = t$ et $\overline{\delta}_1 = \overline{\delta}_2 \in F^\times / N_{L_t/F}(L_t^\times)$
(2) $t_1 = t, t_2 = -t$ et $\overline{\delta}_1 = -\overline{\delta}_2 \in F^\times / N_{L_t/F}(L_t^\times)$.

Bref:

Théorème 3.1. *Soit F un corps de caractéristique différente de 2.*

Alors, toute classe de $\mathrm{PSL}_2(F)$ est de type I+,II,III+ ou IV, et deux classes de types différents ne sont pas conjuguées.

Soit $\overline{M} \in \mathrm{PSL}_2(F)$. Alors :

(1) *$\overline{I}_2$ est l'unique élément de type I+*

(2) *$\overline{M}$ est de type II si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Delta(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, avec $\lambda \in F \setminus \{0, 1, -1\}$.*

   De plus, pour tous $\lambda_1, \lambda_2 \in F \setminus \{0, 1, -1\}$, $\overline{\Delta(\lambda_1}$ et $\overline{\Delta(\lambda_2)}$ sont conjuguées si et seulement si $\{\lambda_1, \lambda_1^{-1}, -\lambda_1, -\lambda_1^{-1}\} = \{\lambda_2, \lambda_2^{-1}, -\lambda_2, -\lambda_2^{-1}\}$

(3) *$\overline{M}$ est de type III+ si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Theta(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, avec $\alpha \in F^\times$*

   De plus, pour tous $\alpha_1, \alpha_2 \in F^\times$, $\overline{\Theta(\alpha_1)}$ et $\overline{\Theta(\alpha_2)}$ sont conjuguées si et seulement si $\overline{\alpha}_1 = \overline{\alpha}_2 \in F^\times / F^{\times 2}$.

(4) *$\overline{M}$ est de type IV si et seulement si elle est conjuguée à la classe d'une matrice de la forme $\Gamma(t, \delta) = \begin{pmatrix} 0 & -\delta \\ \delta^{-1} & t \end{pmatrix}$, où $\delta \in F^\times$ et $t \in F$ est tel que $X^2 - tX + 1$ soit irréductible sur F.*

   De plus, pour tous $(t_1, \delta_1), (t_2, \delta_2) \in F \times F^\times$, où t_1, t_2 vérifient les conditions requises, $\overline{\Gamma(t_1, \delta_1)}$ et $\overline{\Gamma(t_2, \delta_2)}$ sont conjuguées si et seulement s 'il existe $t \in F^\times$ vérifiant une des deux conditions suivantes :

(1) $t_1 = t, t_2 = t$ *et* $\overline{\delta}_1 = \overline{\delta}_2 \in F^\times/N_{L_t/F}(L_t^\times)$
(2) $t_1 = t, t_2 = -t$ *et* $\overline{\delta}_1 = -\overline{\delta}_2 \in F^\times/N_{L_t/F}(L_t^\times)$.

Nous allons maintenant appliquer ce résultat au cas d'un corps fini. Avant toute chose, on a besoin de deux lemmes.

Lemme 3.2. *Soit F un corps fini de caractéristique différent de 2, et soit $M \in \mathrm{SL}_2(F)$. On note* $\mathrm{Conj}(\overline{M})$ *la classe de conjugaison de $\overline{M}$ dans* $\mathrm{PSL}_2(F)$. *Alors, on a*

$$|\mathrm{Conj}(\overline{M})| = \begin{cases} \dfrac{|\mathrm{Conj}(M)|}{2} & \text{si } M \text{ et } -M \text{ sont conjuguées} \\ |\mathrm{Conj}(M)| & \text{sinon.} \end{cases}$$

Démonstration. On va tout d'abord comparer les centralisateurs. Si $P \in \mathrm{SL}_2(F)$, on a $\overline{PM} = \overline{MP}$ si et seulement si $PM = MP$ ou $PM = -MP$.

Si M et $-M$ ne sont pas conjuguées, le second cas ne peut arriver. On a donc $\overline{PM} = \overline{MP}$ si et seulement si $PM = MP$. Comme P et $-P$ ont la même classe dans $\mathrm{PSL}_2(F)$, le centralisateur de $\overline{M}$ possède $\dfrac{|\mathscr{C}_1(M)|}{2}$ éléments. Mais, on a $|\mathrm{PSL}_2(F)| = \dfrac{|\mathrm{SL}_2(F)|}{2}$, et donc $|\mathrm{Conj}(\overline{M})| = |\mathrm{Conj}(M)|$ dans ce cas.

Si $-M = QMQ^{-1}$, avec $Q \in \mathrm{SL}_2(F)$, alors $\overline{PM} = \overline{MP}$ si et seulement si $PM = MP$ ou $Q^{-1}PM = MQ^{-1}P$, c'est-à-dire si et seulement si $P \in \mathscr{C}_1(M) \cup Q\mathscr{C}_1(M)$. Cette dernière réunion étant disjointe, elle possède $2|\mathscr{C}_1(M)|$ éléments, et le centralisateur de $\overline{M}$ possède alors $|\mathscr{C}_1(M)|$ éléments. Par conséquent, $|\mathrm{Conj}(\overline{M})| = \dfrac{|\mathrm{Conj}(M)|}{2}$ dans ce cas. □

Lemme 3.3. *Soit F un corps à q éléments, de caractéristique différente de 2.*

Alors, -1 est un carré dans $F^\times$ si et seulement si $q \equiv 1$ [4].

Démonstration. On remarque que les éléments de $F^{\times 2}$ sont racines du polynôme de $X^{\frac{q-1}{2}} - 1 \in F[X]$, puisque $x^{q-1} = 1$ pour tout $x \in F^\times$ d'après le théorème de Lagrange. Ce polynôme possède donc au moins $\dfrac{q-1}{2}$ racines d'après le lemme 2.4 (1). Comme ce polynôme est de degré $\dfrac{q-1}{2}$, $F^{\times 2}$ est exactement l'ensemble de ses racines et on obtient que, pour tout $x \in F^\times$, on a $x \in F^{\times 2}$ si et seulement si $x^{\frac{q-1}{2}} = 1$.

Le résultat voulu s'obtient alors en prenant $x = -1$. □

On peut maintenant revenir au dénombrement des classes de conjugaison et de leurs cardinaux. D'après le lemme 3.2, on doit comprendre entre autres dans quels cas M et $-M$ sont conjuguées dans $\mathrm{SL}_2(F)$.

On commence par le type II. D'après le théorème précédent, le nombre de classes de conjugaison est égale au nombre de parties de $F \setminus \{0, 1, -1\}$ qui sont de la forme $\{\lambda, \lambda^{-1}, -\lambda, -\lambda^{-1}\}$.

Remarquons que l'égalité $\lambda = \lambda^{-1}$ ne peut se produire puisque $\lambda \neq \pm 1$. L'ensmeble précédent possède donc strictement moins de quatre éléments si et seulement si $\lambda = -\lambda^{-1}$, ce qui équivaut à dire que $-1 \in F^{\times 2}$. Dans ce cas, cet ensemble possède exactement deux éléments, à savoir i et $-i$, où $i \in F^\times$ vérifie $i^2 = -1$.

Autrement dit, si m est le nombre d'ensembles à quatre éléments de la forme précédente, et en tenant compte du lemme précédent, on a

$$|F \setminus \{0, 1, -1\}| = q - 3 = \begin{cases} 4m & \text{si } q \equiv 3\ [4] \\ 4m + 2 & \text{si } q \equiv 1\ [4] \end{cases}$$

Par conséquent, le nombre de classes de conjugaison est $\dfrac{q-3}{4}$ si $q \equiv 3\ [4]$ et $\dfrac{q-5}{4} + 1 = \dfrac{q-1}{4}$ si $q \equiv 1\ [4]$.

Calculons maintenant le cardinal de chaque classe. On commence par déterminer sous quelles conditions $\Delta(\lambda)$ et $-\Delta(\lambda)$ sont conjuguées dans $\mathrm{SL}_2(F)$. D'après le théorème 2.1, cela revient à avoir l'égalité $\{\lambda, \lambda^{-1}\} = \{-\lambda, -\lambda^{-1}\}$. On vérifie que cela équivaut à nouveau à $\lambda^2 = -1$, c'est-à-dire $\{\lambda, \lambda^{-1}\} = \{i, -i\}$.

Ainsi, si $q \equiv 3\ [4]$, chaque classe de conjugaison possède $q(q+1)$ éléments d'après le lemme 3.2 et le théorème 2.5. Si $q \equiv 1[4]$, chaque classe de conjugaison possède $q(q+1)$ éléments, sauf une, qui en possède $\dfrac{q(q+1)}{2}$.

Passons au type III+. Comme on l'a déjà constaté, il y a autant de classes de conjugaison de type III+ dans $\mathrm{PSL}_2(F)$ que dans $\mathrm{SL}_2(F)$. Comme de plus une matrice M de type III+ n'étant jamais conjuguée à $-M$, les classes de conjugaison ont également le même cardinal.

Il reste à considérer le cas du type IV. Le théorème 3.1 et le lemme 2.4 (2) montrent qu'il y a autant de classes de conjugaison que de parties de $F \setminus \mathrm{Im}(\gamma)$ de la forme $\{t, -t\}$. Cet ensemble est réduit à un singleton si et seulement si $0 \in F \setminus \mathrm{Im}(\gamma)$, c'est-à-dire si et seulement si $X^2 + 1$ est irréductible sur F. Cela revient à demander que -1 ne soit pas un carré, c'est-à-dire $q \equiv 3\ [4]$.

D'après le théorème 2.1, $F \setminus \mathrm{Im}(\gamma)$ possède $\dfrac{q-1}{2}$ éléments.

Si $q \equiv 1\ [4]$, il y a donc $\dfrac{q-1}{4}$ classes de conjugaison. Si $q \equiv 3\ [4]$, il y en a $\dfrac{q-3}{4} + 1 = \dfrac{q+1}{4}$.

De plus, les matrices $\Gamma(t,\delta)$ et $-\Gamma(t,\delta) = \Gamma(-t,-\delta)$ sont conjuguées si et seulement si $t = -t$, i.e. $t = 0$. Cela se produit uniquement si $q \equiv 3$ [4], comme vu précédemment.

Par conséquent, si $q \equiv 1$ [4], chaque classe de conjugaison possède $q(q-1)$ d'après le théorème 2.5. Si $q \equiv 3$[4], chaque classe de conjugaison possède $q(q-1)$ éléments, sauf une, qui en possède $\dfrac{q(q-1)}{2}$.

On a donc le théorème suivant.

Théorème 3.4. *Soit F un corps à q éléments, de caractéristique différente de 2 (i.e. q est impair).*

Alors, tout élément de $\mathrm{PSL}_2(F)$ est de type $I+, II, III+$ ou IV, et deux éléments de types différents ne sont pas conjugués.

Si $q \equiv 1$[4], alors :

(1) *il y a 1 classe de conjugaison d'élément de type I+, possédant 1 élément*

(2) *il y a $\dfrac{q-1}{4}$ classes de conjugaison d'éléments de type II: $\dfrac{q-5}{4}$ classes de cardinal $q(q+1)$ et 1 classe de cardinal $\dfrac{q(q+1)}{2}$*

(3) *il y a 2 classes de conjugaison d'éléments de type III+, chacune possédant $\dfrac{(q-1)(q+1)}{2}$ éléments*

(4) *il y a $\dfrac{q-1}{4}$ classes de conjugaison de matrices de type IV, chacune possédant $q(q-1)$ éléments.*

Si $q \equiv 3$[4], alors :

(1) *il y a 1 classe de conjugaison d'élément de type I+, possédant 1 élément*

(2) *il y a $\dfrac{q-3}{4}$ classes de conjugaison d'éléments de type II, chacune possédant $q(q+1)$ éléments*

(3) *il y a 2 classes de conjugaison d'éléments de type III+, chacune possédant $\dfrac{(q-1)(q+1)}{2}$ éléments*

(4) *il y a $\dfrac{q+1}{4}$ classes de conjugaison de matrices de type IV: $\dfrac{q-3}{4}$ classes de cardinal $q(q-1)$ et 1 classe de cardinal $\dfrac{q(q-1)}{2}$*

Au total, $\mathrm{PSL}_2(F)$ possède $\dfrac{q+5}{2}$ classes de conjugaison dans tous les cas.

On continue en donnant un système complet de représentants de classes de conjugaison de $\mathrm{PSL}_2(F)$ lorsque F est un corps fini.

Théorème 3.5. *Soit F un corps à q éléments, où q est impair.*

On suppose que $q \equiv 1$ [4].

Soient Λ et T deux parties de F telles que

$$F = \{0, 1, -1\} \sqcup \{i, -i\} \sqcup \bigsqcup_{\lambda \in \Lambda} \{\lambda, \lambda^{-1}, -\lambda, -\lambda^{-1}\},$$

où $i \in F^\times$ vérifie $i^2 = -1$ et

$$F \setminus \mathrm{Im}(\gamma) = \bigsqcup_{t \in T} \{t, -t\}.$$

On fixe également $\varepsilon \in F^\times \setminus F^{\times 2}$. Alors, les éléments suivants forment un système complet de représentants de classes de conjugaison de $\mathrm{PSL}_2(F)$:

(1) *Type I+: $\overline{I}_2$, dont la classe de conjugaison possède un élément*

(2) *Type II: les $\dfrac{q-5}{2}$ éléments $\overline{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}}$, $\lambda \in \Lambda$, dont les classes de conjugaison possèdent chacune $q(q+1)$ éléments, et $\overline{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}$, dont la classe de conjugaison possède $\dfrac{q(q+1)}{2}$ éléments*

(3) *Type III+: $\overline{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}$, $\overline{\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}}$, dont les classes de conjugaison possèdent chacune $\dfrac{(q-1)(q+1)}{2}$ éléments*

(4) *Type IV: les $\dfrac{q-1}{4}$ éléments $\overline{\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}}$, $t \in T$, dont les classes de conjugaison possèdent chacune $q(q-1)$ éléments.*

On suppose que $q \equiv 3$ [4].

Soient Λ et T deux parties de F telles que

$$F = \{0, 1, -1\} \sqcup \bigsqcup_{\lambda \in \Lambda} \{\lambda, \lambda^{-1}, -\lambda, -\lambda^{-1}\},$$

et

$$F \setminus \mathrm{Im}(\gamma) = \{0\} \sqcup \bigsqcup_{t \in T} \{t, -t\}.$$

Alors, les éléments suivant forment un système complet de représentants de classes de conjugaison de $\mathrm{PSL}_2(F)$:

(1) *Type I+: $\overline{I}_2$, , dont la classe de conjugaison possède un élément*

(2) *Type II: les $\dfrac{q-3}{2}$ éléments $\overline{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}}$, $\lambda \in \Lambda$, dont les classes de conjugaison possèdent chacune $q(q+1)$ éléments*

(3) *Type III+:* $\overline{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}}$, $\overline{\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}}$, , *dont les classes de conjugaison possèdent chacune* $\dfrac{(q-1)(q+1)}{2}$ *éléments*

(4) *Type IV: les* $\dfrac{q-3}{4}$ *éléments* $\overline{\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix}}$, $t \in T$, *dont les classes de conjugaison possèdent chacune* $q(q-1)$ *éléments, et* $\overline{\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}}$, *dont la classe de conjugaison possède* $\dfrac{q(q-1)}{2}$ *éléments.*