Examen Algèbre 1

Responsable : Mr O. DEBARRE

Important : vous pouvez consulter le polycopié et utiliser sans démonstration ses résultats (sauf ceux des exercices ou des TD). Si vous voulez utiliser des résultats hors du cours, il faut les démontrer (sauf mention explicite du contraire).

Exercice 1. Pour chaque entier $n \geq 2$, on considère la forme quadratique

$$f_n(x_1, \ldots, x_n) = x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1$$

sur $\mathbf{R}^n$.

a) Pour chaque $n \in \{2, 3, 4, 5\}$, décomposer f_n en combinaison linéaire de carrés de formes linéaires indépendantes.

b) Déterminer la signature et le rang de f_n pour tout $n \geq 2$.

Exercice 2. Soit V un espace vectoriel réel de dimension finie n, soit V^* son dual, et soit ω un élément de $\bigwedge^2 V^*$.

a) Montrer qu'il existe des éléments $e_1, \ldots, e_{2r}$ de V^* formant une famille libre tels que

$$\omega = e_1 \wedge e_2 + \cdots + e_{2r-1} \wedge e_{2r}$$

(*Indication* : on pourra considérer, en le justifiant, ω comme une forme bilinéaire alternée sur V).

b) En déduire que ω est *décomposable* (c'est-à-dire que ω peut s'écrire $x \wedge y$) si et seulement si

$$\forall \alpha \in \bigwedge^{n-4} V^* \qquad \omega \wedge \omega \wedge \alpha = 0.$$

Exercice 3. On considère la représentation de permutation du groupe $\mathfrak{S}_n$ dans l'espace vectoriel $\mathbf{C}^n$, que l'on décompose en somme de deux sous-représentations : la droite engendrée par le vecteur $(1, \ldots, 1)$ et l'hyperplan

$$V_0 = \{(x_1, \ldots, x_n) \in V \mid x_1 + \cdots + x_n = 0\}.$$

Il est montré dans le polycopié (on ne le redémontrera donc pas) que V_0 est une représentation irréductible de $\mathfrak{S}_n$.

Le but de cet exercice est de montrer que si $n \geq 4$, c'est encore une représentation irréductible du groupe alterné $\mathfrak{A}_n$. On procède par contradiction, en supposant qu'il existe un sous-espace vectoriel $W \subset V_0$ stable par $\mathfrak{A}_n$, non nul et distinct de V_0.

a) Soit $\tau \in \mathfrak{S}_n$ la transposition (12). Montrer que $W + \tau(W)$ et $W \cap \tau(W)$ sont des sous-espaces stables par $\mathfrak{S}_n$. En déduire $V_0 = W \oplus \tau(W)$.

b) Montrer que si $\dim(W) \geq 2$, il existe un vecteur $x = (x_1, \ldots, x_n)$ non nul dans W tel que $x_1 = x_2$. Conclure.

Exercice 4. Dans tout cet exercice, p est un nombre premier *impair*.

a) Montrer qu'il existe $\mu \in \mathbf{F}_p$ qui n'est pas un carré.

T.S.V.P.

b) Calculer le cardinal du groupe $\mathrm{SL}_2(\mathbf{F}_p)$.

c) Exhiber un p-sous-groupe de Sylow de $\mathrm{SL}_2(\mathbf{F}_p)$.

d) Combien $\mathrm{SL}_2(\mathbf{F}_p)$ a-t-il de p-sous-groupes de Sylow ?

e) Soit $M \in \mathrm{SL}_2(\mathbf{F}_p)$ une matrice dont les deux valeurs propres (peut-être confondues) sont dans $\mathbf{F}_p$. Montrer que M est conjuguée, *dans* $\mathrm{SL}_2(\mathbf{F}_p)$, à l'une des matrices suivantes

$$U(a) := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ (a \in \mathbf{F}_p) \quad , \quad -U(a) \quad , \quad D(\lambda) := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \ (\lambda \in \mathbf{F}_p^\times).$$

f) Montrer que les matrices $D(\lambda)$ et $D(\mu)$ sont conjuguées dans $\mathrm{SL}_2(\mathbf{F}_p)$ si et seulement si $\mu \in \{\lambda, \lambda^{-1}\}$.

g) Montrer que les matrices $U(a)$ et $U(b)$ sont conjuguées dans $\mathrm{SL}_2(\mathbf{F}_p)$ si et seulement s'il existe $c \in \mathbf{F}_p^\times$ tel que $b = ac^2$.

h) En déduire que pour les éléments de $\mathrm{SL}_2(\mathbf{F}_p)$ dont les deux valeurs propres sont dans $\mathbf{F}_p$, on obtient au total exactement $\frac{p-3}{2} + 6$ classes de conjugaison distinctes.

i) Pour tout $a, b \in \mathbf{F}_p$ tels que $a^2 - b^2\mu = 1$, on définit un élément de $\mathrm{SL}_2(\mathbf{F}_p)$ en posant

$$M(a,b) := \begin{pmatrix} a & b\mu \\ b & a \end{pmatrix}.$$

Montrer que $M(a,b)$ et $M(a',b')$ sont conjuguées dans $\mathrm{SL}_2(\mathbf{F}_p)$ si et seulement si $a = a'$ et $b \in \{b', -b'\}$.

j) Montrer qu'on obtient ainsi $\frac{p-1}{2}$ nouvelles classes de conjugaison distinctes.

On admettra qu'on a ainsi obtenu toutes les classes de conjugaison de $\mathrm{SL}_2(\mathbf{F}_p)$ *: il y en a donc au total* $p + 4$.

k) Montrer qu'il existe un morphisme surjectif $\mathrm{SL}_2(\mathbf{F}_3) \to \mathfrak{A}_4$.

l) En déduire les dimensions de toutes les représentations irréductibles complexes de $\mathrm{SL}_2(\mathbf{F}_3)$ (on pourra utiliser sans démonstration le résultat de l'exerc. IV.2.17 du polycopié sur les dimensions des représentations irréductibles de $\mathfrak{A}_4$).

m) Déterminer les dimensions de toutes les représentations irréductibles complexes de $\mathrm{SL}_2(\mathbf{F}_5)$ (on pourra utiliser la table p. 54 du poly et (sans démonstration) le résultat de l'exerc. IV.2.18 du polycopié sur les dimensions des représentations irréductibles de $\mathfrak{A}_5$).

Corrigé de l'examen Algèbre 1

Responsable : Mr O. DEBARRE

Exercice 1. *Pour chaque entier $n \geq 2$, on considère la forme quadratique*

$$f_n(x_1, \ldots, x_n) = x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1$$

sur $\mathbf{R}^n$.
a) Pour chaque $n \in \{2, 3, 4, 5\}$, décomposer f_n en combinaison linéaire de carrés de formes linéaires indépendantes.

Pour $n = 2$, on a $f_2(x_1, x_2) = 2x_1x_2 = \frac{1}{2}((x_1 + x_2)^2 - (x_1 - x_2)^2)$.

Pour $n = 3$, on a $f_3(x_1, x_2, x_3) = (x_1+x_3)(x_2+x_3)-x_3^2 = \frac{1}{4}((x_1+x_2+2x_3)^2-(x_1-x_2)^2)-x_3^2$.

Pour $n = 4$, on a $f_4(x_1, x_2, x_3, x_4) = (x_1 + x_3)(x_2 + x_4) = \frac{1}{4}((x_1 + x_2 + x_3 + x_4)^2 - (x_1 - x_2 + x_3 - x_4)^2)$.

Pour $n = 5$, on a $f_5(x_1, x_2, x_3, x_4, x_5) = (x_1 + x_3)(x_2 + x_5) + x_3x_4 + x_4x_5 - x_3x_5 = \frac{1}{4}((x_1 + x_2 + x_3 + x_5)^2 - (x_1 - x_2 + x_3 - x_5)^2) + (x_3 + x_5)(x_4 - x_5) + x_5^2 = \frac{1}{4}((x_1 + x_2 + x_3 + x_5)^2 - (x_1 - x_2 + x_3 - x_5)^2 + (x_3 + x_4)^2 - (x_3 - x_4 + 2x_5)^2) + x_5^2$.

b) Déterminer la signature et le rang de f_n pour tout $n \geq 2$.

Les signatures de f_2, f_3, f_4, f_5 sont donc $(1, 1), (1, 2), (1, 1), (3, 2)$ et les rangs $2, 3, 2, 5$.

Pour $n \geq 6$, on a $f_n(x_1, \ldots, x_n) = (x_1 + x_3)(x_2 + x_n) + x_3x_4 + \cdots + x_{n-1}x_n - x_3x_n = (x_1+x_3)(x_2+x_n)+(x_3+x_5)(x_4-x_n)+x_5x_6\cdots+x_{n-1}x_n+x_5x_n = (x_1+x_3)(x_2+x_n)+(x_3+x_5)(x_4-x_n)+f_{n-4}(x_5,\ldots,x_n)$.

On a donc $\mathrm{sign}(f_n) = (2, 2) + \mathrm{sign}(f_{n-4})$ et, pour tout $n \geq 2$,

$$\mathrm{sign}(f_n) = \begin{cases} (1,1) + (\frac{n-4}{2}, \frac{n-4}{2}) & \text{si } n \equiv 0 \pmod 4, \\ (3,2) + (\frac{n-5}{2}, \frac{n-5}{2}) & \text{si } n \equiv 1 \pmod 4, \\ (1,1) + (\frac{n-2}{2}, \frac{n-2}{2}) & \text{si } n \equiv 2 \pmod 4, \\ (1,2) + (\frac{n-3}{2}, \frac{n-3}{2}) & \text{si } n \equiv 3 \pmod 4, \end{cases} \quad \text{et} \quad \mathrm{rang}(f_n) = \begin{cases} n-2 & \text{si } n \equiv 0 \pmod 4, \\ n & \text{sinon.} \end{cases}$$

Exercice 2. *Soit V un espace vectoriel réel de dimension finie n, soit V^* son dual, et soit ω un élément de $\bigwedge^2 V^*$.*
a) Montrer qu'il existe des éléments $e_1, \ldots, e_{2r}$ de V^* formant une famille libre tels que

$$\omega = e_1 \wedge e_2 + \cdots + e_{2r-1} \wedge e_{2r}.$$

D'après le cours, on peut voir ω comme une forme bilinéaire alternée sur l'espace vectoriel V. D'après le cours, celui-ci se décompose en somme directe orthogonale $P_1 \oplus \cdots \oplus P_r$ de plans hyperboliques et du noyau de ω. Soit $(v_1, \ldots, v_n)$ une base de V adaptée à cette décomposition, avec $\omega(v_{2i-1}, v_{2i}) = 1$ pour chaque $i \in \{1, \ldots, r\}$. Si $(e_1, \ldots, e_n)$ est la base duale de V, on voit que l'élément $e_1 \wedge e_2 + \cdots + e_{2r-1} \wedge e_{2r}$ de $\bigwedge^2 V$, vu comme forme bilinéaire alternée sur V^*, prend la valeur 1 sur (v_{2i-1}, v_{2i}) pour chaque $i \in \{1, \ldots, r\}$ et 0 sur les autres (v_i, v_j) avec $i < j$. Il est donc égal à ω.

b) En déduire que ω est décomposable *(c'est-à-dire que ω peut s'écrire $x \wedge y$) si et seulement si*

$$\forall \alpha \in \textstyle\bigwedge^{n-4} V^* \qquad \omega \wedge \omega \wedge \alpha = 0.$$

Si $\omega = x \wedge y$, on a bien $\omega \wedge \omega \wedge \alpha = x \wedge y \wedge x \wedge y \wedge \alpha = 0$.

Inversement, on écrit ω comme en a), on complète $e_1, \dots, e_{2r}$ en une base $(e_1, \dots, e_n)$ de V^*, et on prend $\alpha = e_5 \wedge \cdots \wedge e_n$. Si $r \geq 2$, on a, puisque les éléments de $\bigwedge^2 V^*$ commutent entre eux, $\omega \wedge \omega \wedge \alpha = 2e_1 \wedge \cdots \wedge e_n \neq 0$. L'hypothèse entraîne donc $r \leq 1$ et ω est décomposable.

Exercice 3. *On considère la représentation de permutation du groupe $\mathfrak{S}_n$ dans l'espace vectoriel $\mathbf{C}^n$, que l'on décompose en somme de deux sous-représentations : la droite engendrée par le vecteur $(1, \dots, 1)$ et l'hyperplan*

$$V_0 = \{(x_1, \dots, x_n) \in V \mid x_1 + \cdots + x_n = 0\}.$$

Il est montré dans le polycopié (on ne le redémontrera donc pas) que V_0 est une représentation irréductible de $\mathfrak{S}_n$.

Le but de cet exercice est de montrer que si $n \geq 4$, c'est encore une représentation irréductible du groupe alterné $\mathfrak{A}_n$. On procède par contradiction, en supposant qu'il existe un sous-espace vectoriel $W \subset V_0$ stable par $\mathfrak{A}_n$, non nul et distinct de V_0.

a) Soit $\tau \in \mathfrak{S}_n$ la transposition (12). Montrer que $W + \tau(W)$ et $W \cap \tau(W)$ sont des sous-espaces stables par $\mathfrak{S}_n$. En déduire $V_0 = W \oplus \tau(W)$.

Soit $\sigma \in \mathfrak{S}_n$. Pour montrer que $W+\tau(W)$ et $W\cap\tau(W)$ sont stables par σ, il suffit de montrer que W et $\tau(W)$ sont soit laissés stables, soit échangés par σ. Si $\sigma \in \mathfrak{A}_n$, on a $\sigma(W) = W$ et $\sigma(\tau(W)) = \tau(\tau\sigma\tau(W)) = \tau(W)$ puisque $\tau\sigma\tau \in \mathfrak{A}_n$, donc $\tau\sigma\tau(W) = W$. Si $\sigma \notin \mathfrak{A}_n$, on a $\sigma\tau, \tau\sigma \in \mathfrak{A}_n$ donc ces deux permutations laissent stables W. On en déduit $\sigma(W) = \tau((\tau\sigma)(W)) = \tau(W)$ et $\sigma(\tau(W)) = (\sigma\tau)(W) = W$.

Comme $W + \tau(W)$ contient W donc n'est pas 0 et que $W \cap \tau(W)$ est contenu dans W donc n'est pas V_0, le premier est V_0 et le second est 0. On a donc bien $V_0 = W \oplus \tau(W)$.

b) Montrer que si $\dim(W) \geq 2$, il existe un vecteur $x = (x_1, \dots, x_n)$ non nul dans W tel que $x_1 = x_2$. Conclure.

Les $x \in W$ tels que $x_1 = x_2$ forment un sous-espace vectoriel de W de codimension ≤ 1 (c'est le noyau d'une forme linéaire), donc non nul si $\dim(W) \geq 2$. Si x est un tel vecteur, il est invariant par τ donc est dans $W \cap \tau(W)$ qui est nul, ce qui est absurde. On a donc $\dim(W) = 1$ et $n - 1 = \dim(V_0) = 2\dim(W) = 2$, ce qui contredit l'hypothèse $n \geq 4$. On a donc montré que l'existence de W conduit à une contradiction, donc V_0 est une représentation irréductible de $\mathfrak{A}_n$.

Exercice 4. *Dans tout cet exercice, p est un nombre premier* impair.

a) Montrer qu'il existe $\mu \in \mathbf{F}_p$ qui n'est pas un carré.

Le morphisme de groupes $\varphi : (\mathbf{F}_p^\times, \times) \to (\mathbf{F}_p^\times, \times)$ d'élévation au carré est de noyau $\{\pm 1\}$, qui est de cardinal 2 puisque p est impair. Son image, qui est l'ensemble des carrés non nuls, est donc de cardinal $\mathrm{Card}(\mathbf{F}_p^\times)/2 < \mathrm{Card}(\mathbf{F}_p^\times)$. Le morphisme φ n'est donc pas surjectif et il existe $\mu \in \mathbf{F}_p^\times$ qui n'est pas un carré.

b) Calculer le cardinal du groupe $\mathrm{SL}_2(\mathbf{F}_p)$.

Un matrice de $\mathrm{GL}_2(\mathbf{F}_p)$ est déterminée par : sa première colonne, quelconque non nulle (soit $p^2 - 1$ choix) et sa deuxième colonne, non colinéaire à la première (soit $p^2 - p$ choix). Le cardinal de $\mathrm{GL}_2(\mathbf{F}_p)$ est donc $(p^2 - 1)(p^2 - p)$. Le morphisme déterminant $\mathrm{GL}_2(\mathbf{F}_p) \to \mathbf{F}_p^\times$ est surjectif. Son noyau $\mathrm{SL}_2(\mathbf{F}_p)$ est donc de cardinal $\mathrm{Card}(\mathrm{GL}_2(\mathbf{F}_p))/\mathrm{Card}(\mathbf{F}_p^\times) = (p^2-1)(p^2-p)/(p-1) = p(p^2 - 1)$.

c) Exhiber un p-sous-groupe de Sylow de $\mathrm{SL}_2(\mathbf{F}_p)$.

La puissance maximale de p divisant le cardinal de $\mathrm{SL}_2(\mathbf{F}_p)$ est p. Le sous-groupe $\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbf{F}_p\}$ est de cardinal p ; c'est donc un p-sous-groupe de Sylow de $\mathrm{SL}_2(\mathbf{F}_p)$.

d) Combien $\mathrm{SL}_2(\mathbf{F}_p)$ *a-t-il de* p*-sous-groupes de Sylow ?*

Par le théorème de Sylow, le nombre de p-sous-groupes de Sylow s'écrit $rp+1$ et divise p^2-1. On peut donc écrire $p^2-1=(rp+1)m$. On a $m \equiv -1 \pmod p$, donc $m=sp-1$ et $p^2-1=(rp+1)(sp-1)$. Si $r \geq 2$, on écrit $p^2-1=(rp+1)(sp-1) \geq (2p+1)(p-1)$, ce qui est absurde. Si $r=0$, il n'y a qu'un p-sous-groupe de Sylow, ce qui est absurde puisque $\{\left(\begin{smallmatrix}1&0\\a&1\end{smallmatrix}\right) \mid a \in \mathbf{F}_p\}$ en est un autre. On a donc $r=1$ et le nombre de p-sous-groupes de Sylow est $p+1$.

e) Soit $M \in \mathrm{SL}_2(\mathbf{F}_p)$ *une matrice dont les deux valeurs propres (peut-être confondues) sont dans* $\mathbf{F}_p$*. Montrer que* M *est conjuguée,* dans $\mathrm{SL}_2(\mathbf{F}_p)$*, à l'une des matrices suivantes*

$$U(a) := \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \ (a \in \mathbf{F}_p) \quad , \quad -U(a) \quad , \quad D(\lambda) := \begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix} \ (\lambda \in \mathbf{F}_p^\times).$$

Si M a deux valeurs propres distinctes, elle est diagonalisable, donc s'écrit $P^{-1}D(\lambda)P$, avec $\lambda \neq \pm 1$ et P inversible, mais pas nécessairement dans $\mathrm{SL}_2(\mathbf{F}_p)$. Les colonnes de P sont les coordonnées d'une base de vecteurs propres de l'endomorphisme de $\mathbf{F}_p^2$ de matrice M. Si on multiplie la deuxième colonne par $\det(P)^{-1}$, on a encore une base de vecteurs propres mais le déterminant devient 1. La matrice M est donc conjuguée, dans $\mathrm{SL}_2(\mathbf{F}_p)$, à $D(\lambda)$.

Si les deux valeurs propres de M sont égales, comme leur produit vaut 1, elles sont toutes deux égales à 1 ou toutes deux égales à -1. Si e_1 est un vecteur propre pour cette valeur propre et que l'on complète en une base de $\mathbf{F}_p^2$ de déterminant 1, on obtient une matrice $P \in \mathrm{SL}_2(\mathbf{F}_p)$ telle que $PMP^{-1} = \pm U(a)$.

f) Montrer que les matrices $D(\lambda)$ *et* $D(\mu)$ *sont conjuguées dans* $\mathrm{SL}_2(\mathbf{F}_p)$ *si et seulement si* $\mu \in \{\lambda, \lambda^{-1}\}$.

Si les matrices $D(\lambda)$ et $D(\mu)$ sont conjuguées, elles ont mêmes valeurs propres, donc $\mu \in \{\lambda, \lambda^{-1}\}$.

Inversement, si $\mu = \lambda^{-1}$, on a $D(\lambda) = \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right) D(\mu) \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)^{-1}$.

g) Montrer que les matrices $U(a)$ *et* $U(b)$ *sont conjuguées dans* $\mathrm{SL}_2(\mathbf{F}_p)$ *si et seulement s'il existe* $c \in \mathbf{F}_p^\times$ *tel que* $b = ac^2$*.*

Si $U(a)$ et $U(b)$ sont conjuguées dans $\mathrm{SL}_2(\mathbf{F}_p)$, on écrit $U(a)\left(\begin{smallmatrix}\alpha&\beta\\\gamma&\delta\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha&\beta\\\gamma&\delta\end{smallmatrix}\right) U(b)$ avec $\alpha\delta - \beta\gamma = 1$. En calculant (et en supposant $a \neq 0$), on obtient $\gamma = 0$ et $b\alpha = a\delta$ avec $\alpha\delta = 1$, c'est-à-dire $b = a\delta^2$. Cela établit l'équivalence.

h) En déduire que pour les éléments de $\mathrm{SL}_2(\mathbf{F}_p)$ *dont les deux valeurs propres sont dans* $\mathbf{F}_p$*, on obtient au total exactement* $\frac{p-3}{2} + 6$ *classes de conjugaison distinctes.*

Pour les $D(\lambda)$, on a (par la question f)) les classes $\{D(1)\} = \{I_2\}$ et $\{D(-1)\} = \{-I_2\}$, puis les $(p-3)/2$ classes $\{D(\lambda), D(\lambda^{-1})\}$ pour $\lambda \in \mathbf{F}_p^\times \setminus \{\pm 1\}$.

Pour les $U(a)$, avec $a \in \mathbf{F}_p^\times$, on a (par la question g)) deux classes : celle de $U(1)$ et celle de $U(\mu)$.

C'est la même chose pour les $-U(a)$, soit au total $2 + (p-3)/2 + 2 + 2$ classes.

i) Pour tout $a, b \in \mathbf{F}_p$ *tels que* $a^2 - b^2\mu = 1$*, on définit un élément de* $\mathrm{SL}_2(\mathbf{F}_p)$ *en posant*

$$M(a,b) := \begin{pmatrix}a & b\mu\\ b & a\end{pmatrix}.$$

Montrer que $M(a,b)$ *et* $M(a',b')$ *sont conjuguées dans* $\mathrm{SL}_2(\mathbf{F}_p)$ *si et seulement si* $a = a'$ *et* $b \in \{b', -b'\}$.

La trace de $M(a,b)$ est $2a$. Si $M(a,b)$ et $M(a',b')$ sont conjuguées, elle ont même trace, donc $a=a'$ (puisque la caractéristique est $\neq 2$) ; cela entraîne $b^2=(a^2-1)/\mu=b'^2$, donc $b\in\{b',-b'\}$.

Inversement, il faut montrer que $M(a,b)$ et $M(a,-b)$ (avec $b\neq 0$) sont conjuguées dans $\mathrm{SL}_2(\mathbf{F}_p)$. On écrit $M(a,b)\left(\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right)=\left(\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right)M(a,-b)$ avec $\alpha\delta-\beta\gamma=1$. En calculant, on obtient que c'est équivalent à $\alpha=-\delta$ et $\beta=-\mu\gamma$, avec $-\alpha^2+\mu\gamma^2=1$. Pour montrer qu'il existe un tel couple (α,β), on compte : l'ensemble $\{\mu\gamma^2-1\mid\gamma\in\mathbf{F}_p\}$ a autant d'éléments qu'il y a de carrés dans $\mathbf{F}_p$, c'est-à-dire $(p+1)/2$. Il rencontre donc l'ensemble à $(p+1)/2$ éléments des carrés : il existe γ et α tels que $\mu\gamma^2-1=\alpha^2$.

j) Montrer qu'on obtient ainsi $\frac{p-1}{2}$ nouvelles classes de conjugaison distinctes.

Il faut calculer le cardinal de $\mathscr{A}:=\{(a,b)\in\mathbf{F}_p^2\mid a^2-b^2\mu=1\}$. Si $a=1$, on a $b=0$; si $a\neq 1$, on pose $t:=b/(a-1)$. La condition est équivalente à $a^2-1=b^2\mu=t^2(a-1)^2\mu$, ou $a+1=t^2(a-1)\mu$, soit $a=\frac{t^2\mu+1}{t^2\mu-1}$ et $b=t(a-1)$. Cela signifie que l'application $(a,b)\mapsto b/(a-1)$ induit une bijection entre $\mathscr{A}\setminus\{(1,0)\}$ et $\mathbf{F}_p$ (le dénominateur $t^2\mu-1$ n'est jamais nul puisque μ n'est pas un carré). On a donc $\mathrm{Card}(\mathscr{A})=p+1$.

Il faut retirer de $\mathscr{A}$ les deux points $(\pm1,0)$ (puisque les $M(\pm1,0)=\pm I_2$ ont déjà été comptées). On obtient ainsi (par la question i)) $\frac{p-1}{2}$ nouvelles classes.

On admettra qu'on a ainsi obtenu toutes les classes de conjugaison de $\mathrm{SL}_2(\mathbf{F}_p)$: il y en a donc au total $p+4$.

k) Montrer qu'il existe un morphisme surjectif $\mathrm{SL}_2(\mathbf{F}_3)\to\mathfrak{A}_4$.

L'action de $\mathrm{SL}_2(\mathbf{F}_3)$ sur $\mathbf{P}^1(\mathbf{F}_3)$, qui est un ensemble à 4 éléments, induit un morphisme de groupes $\mathrm{SL}_2(\mathbf{F}_3)\to\mathfrak{S}_4$ dont on a vu en cours que le noyau est $\{\pm I_2\}$. Son image H est donc de cardinal $\mathrm{Card}(\mathrm{SL}_2(\mathbf{F}_3))/2=3(3^2-1)/2=12$ donc d'indice 2 dans $\mathfrak{S}_4$. Elle est donc distinguée dans $\mathfrak{S}_4$ et $\mathfrak{S}_4/H$ est d'ordre 2 donc abélien. Le groupe dérivé $D(\mathfrak{S}_4)=\mathfrak{A}_4$ est donc contenu dans H ; comme ils ont même cardinal, ils sont égaux.

l) En déduire les dimensions de toutes les représentations irréductibles complexes de $\mathrm{SL}_2(\mathbf{F}_3)$.

Comme $\mathfrak{A}_4$ a trois représentations irréductibles de dimension 1 et une de dimension 3 (exerc. IV.2.17), $\mathrm{SL}_2(\mathbf{F}_3)$ aussi. Il a au total 7 représentations irréductibles, de dimension $1,1,1,3,n_1,n_2,n_3$, avec $1^2+1^2+1^2+3^2+n_1^2+n_2^2+n_3^2=\mathrm{Card}(\mathrm{SL}_2(\mathbf{F}_3))=24$, soit $n_1^2+n_2^2+n_3^2=12$. On voit facilement que la seule solution est $2,2,2$.

m) Déterminer les dimensions de toutes les représentations irréductibles complexes de $\mathrm{SL}_2(\mathbf{F}_5)$.

Le groupe $\mathrm{PSL}_2(\mathbf{F}_5)$ est isomorphe à $\mathscr{A}_5$; il existe donc un morphisme surjectif $\mathrm{SL}_2(\mathbf{F}_5)\to\mathscr{A}_5$. Tout comme $\mathfrak{A}_5$ (exerc. IV.2.18), le groupe $\mathrm{SL}_2(\mathbf{F}_3)$ a donc des représentations irréductibles de dimension 1, 3, 3, 4, 5.

Il a au total 9 représentations irréductibles, de dimension $1,3,3,4,5,n_1,n_2,n_3,n_4$, avec $1^2+3^2+3^2+4^2+5^2+n_1^2+n_2^2+n_3^2+n_4^2=\mathrm{Card}(\mathrm{SL}_2(\mathbf{F}_5))=120$, soit $n_1^2+n_2^2+n_3^2+n_4^2=60$. On vérifie que les seules solutions sont $2,2,4,6$ et $1,1,3,7$. Pour exclure la deuxième possibilité, on peut soit invoquer le théorème qui dit que les dimensions des représentations irréductibles divisent l'ordre du groupe (c'est-à-dire 120), soit dire que les représentations de dimension 1 se factorisent par le quotient de $\mathrm{SL}_2(\mathbf{F}_5)$ par son groupe dérivé ; comme celui-ci est $\mathrm{SL}_2(\mathbf{F}_5)$ (th. II.2.6 du poly), la seule représentation de dimension 1 est triviale, donc tous les n_i sont >1.