

## RAPPELS ET EXERCICES SUR LE GROUPE LINÉAIRE I - CORRECTION

### 1 Le groupe linéaire, définition

**Exercice 1.** Par définition, l'isomorphisme  $\varphi_{\mathcal{B}}$  envoie un vecteur  $x \in E$  sur un vecteur  $x_{\mathcal{B}} \in k^n$ , qui est donné par les coordonnées de  $x$  dans la base  $\mathcal{B}$ .

1. Soit  $f : E \rightarrow E$  un isomorphisme vectoriel. On pose  $M_{\mathcal{B}}(f) := \varphi_{\mathcal{B}} \circ f \circ \varphi_{\mathcal{B}}^{-1}$ , il s'agit bien d'un automorphisme vectoriel de  $k^n$  comme composée d'isomorphismes. Soit  $v \in k^n$ , il existe un unique  $x \in E$  tel que  $\varphi_{\mathcal{B}}(x) = v$ , le vecteur  $M_{\mathcal{B}}(f).v$  est alors donné par les coordonnées de  $f(x)$  dans la base  $\mathcal{B}$  :  $M_{\mathcal{B}}(f)$  est la matrice de  $f$  dans la base  $\mathcal{B}$ .

2. On a

$$M_{\mathcal{B}'}(f) = \varphi_{\mathcal{B}'} \circ f \circ \varphi_{\mathcal{B}'}^{-1} = \varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1} \varphi_{\mathcal{B}} \circ f \circ \varphi_{\mathcal{B}}^{-1} \varphi_{\mathcal{B}} \circ \varphi_{\mathcal{B}'}^{-1} = (\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1}) \circ M_{\mathcal{B}}(f) \circ (\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1})^{-1}$$

Donc  $M_{\mathcal{B}'}(f)$  est la conjuguée de la matrice  $M_{\mathcal{B}}(f)$  par l'automorphisme  $(\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1})$ , qui n'est nul autre que le changement de base de  $\mathcal{B}$  vers  $\mathcal{B}'$ .

3. Soient  $\mathcal{B}$  et  $\mathcal{B}'$  deux bases de  $E$ . Par la question précédente, on a

$$\begin{aligned} \det(M_{\mathcal{B}'}(f)) &= \det((\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1}) \circ M_{\mathcal{B}}(f) \circ (\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1})^{-1}) \\ &= \det(\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1}) \det M_{\mathcal{B}}(f) \det((\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1})^{-1}) \\ &= \det(\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1}) \det(\varphi_{\mathcal{B}'} \circ \varphi_{\mathcal{B}}^{-1})^{-1} \det M_{\mathcal{B}}(f) \\ &= \det M_{\mathcal{B}}(f) \end{aligned}$$

D'où le résultat : les déterminants des deux matrices  $M_{\mathcal{B}'}(f)$  et  $M_{\mathcal{B}}(f)$  sont égaux.

**Exercice 2.**

1. Soit  $\lambda \in k^*$ , on pose

$$\iota(\lambda) := \begin{pmatrix} \lambda & 0 \\ 0 & I_{n-1} \end{pmatrix}$$

Cette matrice est bien-sûr inversible  $\iota(\lambda)^{-1} = \iota(\lambda^{-1})$ , et comme elle est diagonale, on trouve immédiatement  $\iota(\lambda\mu) = \iota(\lambda)\iota(\mu)$  pour  $\lambda, \mu \in k^*$ . De même, le fait que  $\iota(\lambda)$  soit diagonale donne  $\det(\iota(\lambda)) = \lambda$ , donc  $\iota$  forme bien une section de  $\det$ .

2. C'est une des caractérisations du produit semi-direct : l'existence d'une section dans une suite exacte courte. De façon équivalente, on pose  $N = \text{SL}(E)$ , et  $H = \iota(k^\times)$ . On a deux sous groupes de  $\text{GL}(E)$ , avec  $N \triangleleft \text{GL}(E)$ ,  $N \cap H = \{\text{Id}_E\}$  car le déterminant de  $\iota(\lambda) = \lambda$ , et  $NH = \text{GL}(E)$  (pour  $u \in \text{GL}(E)$ , on a  $u = \iota(\det(u))\iota(\det(u)^{-1})u$ ).

**Exercice 3.** Cet exercice est en fait un exercice de dénombrement des bases. Commençons par noter qu'une matrice de  $\text{GL}_n(k)$  est équivalente à la donnée d'une base de  $k^n$ , la base formée par ses colonnes (il s'agit bien d'une base par définition du déterminant !). On rappelle que le cardinal d'un  $\mathbb{F}_q$ -espace vectoriel de dimension  $m$  est  $q^m$ .

- On doit d'abord choisir le premier vecteur de notre base : tout vecteur sauf le vecteur nul convient. Il y a donc  $q^n - 1$  choix possibles.
- Supposons que les  $i$ -premiers vecteurs aient déjà été choisis (pour  $1 \leq i < n$ ). Le  $i + 1$ -ème vecteur doit ne pas se trouver dans l'espace engendré par les  $i$  premiers (pour former au total une famille libre), il y a donc  $q^n - q^i$  choix possibles.

Au total, le nombre de choix possibles pour une base est donné par le produit suivant :

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

Comme  $q^n - q^i = q^i(q^{n-i} - 1)$ , on obtient également

$$|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1) \dots (q^2 - 1)(q - 1).$$

La suite exacte courte de l'exercice précédent nous apprend que  $\mathrm{SL}_n(k)$  est d'indice  $|k^*|$  dans  $\mathrm{GL}_n(k)$ . En l'occurrence,  $\mathrm{SL}_n(\mathbb{F}_q)$  est d'indice  $q - 1$  dans  $\mathrm{GL}_n(\mathbb{F}_q)$ , d'où

$$|\mathrm{SL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1) \dots (q^2 - 1).$$

Autre méthode : On peut faire agir  $\mathrm{GL}_n(\mathbb{F}_q)$  sur  $(\mathbb{F}_q)^n$ . En utilisant la formule des classes, on obtient la relation de récurrence suivante

$$\forall n \geq 2, |\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)|\mathbb{F}_q^{n-1}| |\mathrm{GL}_{n-1}(\mathbb{F}_q)|$$

Qui permet aussi de démontrer le résultat.

## 2 Un système de générateurs

**Exercice 4.** La matrice  $\delta(\lambda)$  est diagonale, on a donc

$$\forall n \in \mathbb{N}, \delta(\lambda)^n = \begin{pmatrix} 1 & 0 \\ 0 & \lambda^n \end{pmatrix}$$

Cette matrice est égale à  $I_2$  si et seulement si  $\lambda^n = 1$ . L'ordre de  $\delta(\lambda)$  est donc égal à celui de  $\lambda$  (en particulier, il est infini si  $\lambda$  est d'ordre infini dans  $k^*$ ).

Ensuite, on a pour  $n \in \mathbb{N}$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

On en déduit par récurrence que  $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ , ainsi,  $T^n = I_2$  si et seulement si  $n = 0$  dans  $k$ , autrement dit si  $\mathrm{car}(k) | n$ . Si  $\mathrm{car}(k) = 0$ , alors  $T$  est d'ordre infini, autrement elle est d'ordre  $\mathrm{car}(k)$ .

**Exercice 5.** (Dilatations)

(i)  $\Rightarrow$  (ii) Par contraposée : si toutes les valeurs propres de  $u$  sont égales à 1, alors il en va de même de son déterminant, qui est le produit de ses valeurs propres.

(ii)  $\Rightarrow$  (i) Par hypothèse, comme  $u$  fixe un hyperplan, 1 est une valeur propre de  $u$  de multiplicité au moins  $n - 1$ . Si  $\lambda \neq 1$  est une autre valeur propre de  $u$ , le déterminant de  $u$  est donné par  $1^{n-1}\lambda = \lambda \neq 1$ .

(ii)  $\Rightarrow$  (iii) Par hypothèse, il existe un vecteur propre  $x$  tel que  $u(x) = \lambda x$  avec  $\lambda \neq 1$ . On considère  $u(x) - x = (\lambda - 1)x \in \mathrm{Im}(u - \mathrm{Id})$ . Il s'agit d'un vecteur propre pour la valeur propre  $\lambda \neq 1$ , donc  $(\lambda - 1)x \notin H$  et  $\mathrm{Im}(u - \mathrm{Id}) \not\subset H$ .

(iii)  $\Rightarrow$  (ii) Il existe par hypothèse un vecteur  $x \in \mathrm{Im}(u - \mathrm{Id})$  qui n'est pas dans  $H$ . Par le théorème du rang, on sait que  $\mathrm{Im}(u - \mathrm{Id})$  est une droite (car  $\ker(u - \mathrm{Id})$  est un hyperplan). Donc  $\mathrm{Im}(u - \mathrm{Id})$  est en fait engendrée par  $x$ . Il existe donc un certain  $\mu \in k^*$  tel que  $u(x) - x = \mu x$  (et  $\mu \neq 0$  car  $x \notin H$ ). On a donc  $u(x) = (\mu + 1)x$  et  $\lambda = \mu + 1$  est une valeur propre de  $u$  différente de 1.

(iv)  $\Rightarrow$  (ii) est immédiat.

(ii)  $\Rightarrow$  (iv) Si  $\lambda \neq 1$  est une valeur propre de  $u$ , alors les deux espaces propres  $\mathrm{Ker}(u - \mathrm{Id})$  et  $\mathrm{Ker}(u - \lambda \mathrm{Id})$  sont en somme directe, et la somme de leurs dimensions est  $n - 1 + 1 = n$ . L'endomorphisme  $u$  est donc diagonalisable, et sa forme dans une base de diagonalisation est bien la forme donnée dans (iv).

**Exercice 6.** (Transvections)

On commence par noter que  $(1) \Leftrightarrow \neg(i)$  et  $(3) \Leftrightarrow \neg(i)$  par construction. Ensuite, l'implication  $(ii) \Rightarrow (iv)$  obtenue à l'exercice précédent donne en particulier  $(ii) \Rightarrow \neg(2)$ . Réciproquement, si on a  $\neg(2)$ , alors on peut diagonaliser  $u$ , on a alors  $(ii)$  car le seul endomorphisme diagonalisable dont toutes les valeurs propres sont égales à 1 est  $\text{Id}$  et on a  $u \neq \text{Id}$  par hypothèse.

L'équivalence  $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$  démontrée dans l'exercice précédent nous donne donc directement l'équivalence  $(1) \Leftrightarrow (2) \Leftrightarrow (3)$ .

$(iii) \Rightarrow (iv)$  Comme  $f$  est non identiquement nulle, on peut choisir un  $x_0 \in E$  tel que  $f(x_0) = 1$ . La droite  $\text{Vect}(x_0)$  est un supplémentaire de  $H$  dans  $E$ . On pose  $a := u(x_0) - x_0 \in H \setminus \{0\}$ . Tout élément  $x \in E$  s'écrit de manière unique sous la forme  $x_h + \lambda x_0$  avec  $x_h \in H$  et  $\lambda \in k$ . On a

$$f(x) = f(x_h + \lambda x_0) = \lambda f(x_0) = \lambda$$

Donc  $x = x_h + f(x)x_0$  et on a

$$u(x) = u(x_h) + f(x)u(x_0) = x_h + f(x)x_0 - f(x)x_0 + f(x)u(x_0) = x + f(x)a$$

d'où  $(iv)$ .

$(iv) \Rightarrow (v)$  On complète  $a$  en une base  $v_1, \dots, v_{n-2}, a$  de  $H$ . On prend ensuite  $x_0$  tel que  $f(x_0) = 1$ . On a ainsi une base  $v_1, \dots, v_{n-2}, a, x_0$  de  $E$ , et

$$u(x_0) = x_0 + f(x_0)a = x_0 + a$$

La forme de  $u$  dans la base ainsi construite est donc bien la forme souhaitée.

$(v) \Rightarrow (iii)$  est évident d'après la forme de la matrice.

**Exercice 7.**

1. Soient  $f, f' \in E^*$  et  $a, a'$  non nuls et dans les noyaux respectifs de  $f$  et  $f'$ . On suppose que

$$\forall x \in E, \tau(f, a)(x) = \tau(f', a')(x).$$

On a donc en particulier  $f(x)a = f'(x)a'$  pour tout  $x \in E$ . Comme  $a$  et  $a'$  sont non nuls, on a

$$\forall x \in E, f(x) = 0 \Leftrightarrow f(x)a = 0 = f'(x)a' \Leftrightarrow f'(x) = 0.$$

Donc  $\text{Ker } f = \text{Ker } f'$ , et il existe  $\lambda \in k^*$  tel que  $f' = \lambda f$ . On a alors  $f(x)a = \lambda f(x)a'$  pour tout  $x \in E$ . En prenant  $x$  tel que  $f(x) = 1$  (c'est possible car  $f \in E^* \setminus \{0\}$ ), on trouve que  $a = \lambda a'$  et  $\lambda^{-1}a = a'$ .

Réciproquement, pour  $\lambda \in k^*$  et  $x \in E$ , on a

$$\tau(\lambda f, \lambda^{-1}a) = x + \lambda f(x)\lambda^{-1}a = x + f(x)a = \tau(f, a)$$

D'où l'équivalence voulue.

Une conséquence : Ce résultat peut servir à dénombrer les transvections. Considérons l'ensemble

$$Y = \{(f, a) \in E^* \times E \mid f \neq 0, a \neq 0 \text{ et } f(a) = 0\}.$$

On a une action de  $k^*$  sur  $Y$ , donnée par  $\lambda.(f, a) = (\lambda f, \lambda^{-1}a)$ , et une application  $(f, a) \mapsto \tau(f, a)$ , qui met en bijection les orbites de  $Y$  sous l'action de  $k$  et les transvections. L'action de  $k^*$  sur  $Y$  est libre (les stabilisateurs sont tous triviaux).

Si  $|k| = q$ , alors il y a  $|Y|/(q-1)$  transvections. Maintenant, quelle que soit  $f \in E^*$ , l'ensemble des  $a$  non nuls tels que  $f(a) = 0$  est en bijection avec  $k^{n-1} \setminus \{0\}$  (hyperplan). Donc  $Y$  est en bijection avec  $(k^n \setminus \{0\}) \times (k^{n-1} \setminus \{0\})$ .

Il y a donc

$$\frac{(q^n - 1)(q^{n-1} - 1)}{q - 1} = (q^{n-1} - 1)(1 + q + \dots + q^{n-1})$$

transvections dans  $\text{GL}_n(\mathbb{F}_q)$ .

2. Soient  $a, b \in \text{Ker } f \setminus \{0\}$ . Pour  $x \in E$ , on a

$$\begin{aligned}\tau(f, a) \circ \tau(f, b)(x) &= \tau(f, a)(x + f(x)b) \\ &= x + f(x)b + f(x + f(x)b)a \\ &= x + f(x)b + f(x)a + f(x)f(b)a \\ &= x + f(x)(a + b)\end{aligned}$$

Si  $a + b \neq 0$ , on trouve bien que  $\tau(f, a) \circ \tau(f, b) = \tau(f, a + b)$ . Si  $a + b = 0$ , on trouve  $\tau(f, a) \circ \tau(f, b) = \text{Id}_E$ , d'où le second résultat.

3. Il suffit de montrer que  $\tau(f, a)$  stabilise globalement  $\text{ker } f$ . Soit  $x \in \text{ker } f$ , on a

$$\tau(f, a)(x) = x + f(x)a = x$$

donc  $\tau(f, a)$  fixe même ponctuellement  $\text{ker } f$ . Donc  $\tau(f, a)$  induit un endomorphisme de  $E/\text{ker } f$ , donné par

$$\tau(f, a)(x + \text{ker } f) = \tau(f, a)(x) + \text{ker } f = x + f(x)a + \text{ker } f = x + \text{ker } f.$$

L'endomorphisme de  $E/\text{ker } f$  induit par  $\tau(f, a)$  est donc l'identité de  $E/\text{ker } f$ .

4. Soit  $x \in E$ , on a

$$\begin{aligned}u \circ \tau(f, a) \circ u^{-1}(x) &= u(u^{-1}(x) + f(u^{-1}(x))a) \\ &= x + f(u^{-1}(x))u(a) \\ &= \tau(f \circ u^{-1}, u(a))\end{aligned}$$

L'hyperplan de cette transvection est  $\text{ker}(f \circ u^{-1}) = u(\text{ker } f)$ . Sa droite est  $\text{Vect}(u(a)) = u(\text{Vect}(a))$ .

### 3 Sous-groupes remarquables

#### 3.1 Centres, groupes projectifs

##### Exercice 8.

1. Par hypothèse, il existe pour tout  $x \in E$  un scalaire  $\lambda_x$  tel que  $u(x) = \lambda_x x$ . Comme  $u \in \text{GL}(E)$ , on sait que  $\lambda_x \neq 0$  si  $x \neq 0$ .

Si  $x$  et  $y$  sont deux vecteurs non nuls et colinéaires, on a  $y = \mu x$  pour un  $x \neq 0$ . On a alors

$$\lambda_y y = \lambda_y \mu x = u(y) = \mu(u(x)) = \mu \lambda_x x.$$

Comme  $x$  et  $\mu$  sont non nuls, on en déduit que  $\lambda_x = \lambda_y$ .

Si  $x$  et  $y$  sont non colinéaires, ils forment une base de  $\text{Vect}(x, y)$ . Or on a

$$\lambda_x x + \lambda_y y = u(x) + u(y) = u(x + y) = \lambda_{x+y}(x + y) = \lambda_{x+y}x + \lambda_{x+y}y.$$

donc  $\lambda_{x+y} = \lambda_x = \lambda_y$ .

Ainsi, la valeur de  $\lambda_x$  ne dépend pas de  $x \neq 0$ , et  $\lambda_0$  peut prendre n'importe quelle valeur : il existe  $\lambda \neq 0$  tel que  $u(x) = \lambda x$  pour tout  $x \in E$  et  $u$  est une homothétie.

2. Soit  $D = \text{Vect}(a)$  une droite de  $E$ , et soit  $H = \text{ker } f$  un hyperplan contenant  $D$ . Dire que  $u$  commute avec la transvection  $\tau(f, a)$  donne en particulier  $u(H) = H$  et  $u(D) = D$  d'après l'exercice 7. Ceci étant vrai pour toute droite  $D$ , on conclut que  $u$  est une homothétie d'après la question précédente.

3. Soit  $u \in Z(\text{GL}(E))$ , on a que  $u$  commute en particulier avec toutes les transvections, il s'agit donc d'une homothétie. De même pour  $u \in Z(\text{SL}(E))$  étant donné que  $\text{SL}(E)$  contient également toutes les transvections. Les homothéties faisant clairement partie du centre de  $\text{GL}(E)$ , on a bien le résultat voulu.

**Exercice 9.**

1. Le groupe  $Z(\mathrm{GL}(E))$  est isomorphe à  $k^*$  (par le choix du rapport de l'homothétie), on a donc

$$|\mathrm{PGL}_n(\mathbb{F}_q)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathbb{F}_q^*|} = |\mathrm{SL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n - 1) \dots (q^2 - 1)$$

de même, on a

$$|\mathrm{PSL}_n(\mathbb{F}_q)| = \frac{|\mathrm{SL}_n(\mathbb{F}_q)|}{|\mu_n(k)|} = \frac{1}{|\mu_n(k)|} q^{\frac{n(n-1)}{2}}(q^n - 1) \dots (q^2 - 1)$$

2. Pour  $k = \mathbb{F}_2$ , on a  $k^* = \{1\}$  est le groupe trivial. Donc  $\det$  est trivial sur  $\mathrm{GL}_n(\mathbb{F}_2)$ , qui est donc égal à  $\mathrm{SL}_n(\mathbb{F}_2)$ . De même,  $k^*$  trivial entraîne que les centres de  $\mathrm{GL}_n(\mathbb{F}_2)$  et  $\mathrm{SL}_n(\mathbb{F}_2)$  sont triviaux, d'où le résultat.

**Exercice 10.**

1. Cela découle immédiatement du fait que  $k$  est commutatif : pour  $\lambda, \mu \in k^*$ , on a  $(\lambda\mu)^n = \lambda^n \mu^n$ .

2. Par définition de  $e_n$ , on a

$$e_n(\lambda) = 1 \Leftrightarrow \lambda^n = 1 \Leftrightarrow \lambda \in \mu_n(k)$$

donc  $\ker e_n = \mu_n(k)$ .

3. Dans toute base de  $E$ , la matrice de  $h_\lambda$  est diagonale, et son déterminant est  $\lambda^n$ . On en déduit que l'application  $\det$  est bien définie : soient  $u, v$  deux représentants d'une même classe modulo  $Z(\mathrm{GL}(E))$ , on a  $u = vh_\lambda$  pour un certain  $\lambda$ . Donc  $\det(u) = \det(v) \det(h_\lambda) = \det(v) \lambda^n$ . et  $\det(u) \equiv \det(v)[k^{*n}]$ .

Soit ensuite  $u[Z(\mathrm{GL}(E))] \in \mathrm{PGL}(E)$ . On a  $u[Z(\mathrm{GL}(E))] \in \ker \det$  si et seulement si  $\det(u) \in k^{*n}$ . Dans ce cas, il existe  $\lambda \in k^*$  tel que  $\lambda^n = \det(u)$ . On a  $u = u \circ h_{\lambda^{-1}}$  dans  $\mathrm{PGL}(E)$  et  $u \circ h_{\lambda^{-1}} \in \mathrm{SL}(E)$ , d'où  $u[Z(\mathrm{GL}(E))] \in \mathrm{PSL}(E)$ .

**3.2 Groupe dérivé**

**Exercice 11.** Soit  $\varphi$  un automorphisme de  $E$ , on a

$$\varphi([g, h]) = [\varphi(g), \varphi(h)] \quad \text{et} \quad [g, h] = [\varphi^{-1}(g), \varphi^{-1}(h)]$$

Autrement dit  $\varphi$  induit une bijection de l'ensemble des commutateurs de  $G$ . On en déduit  $\varphi(D(G)) \subset D(G)$  et  $D(G) \subset \varphi(D(G))$ , d'où l'égalité.

Soit ensuite  $g \in G$ , la conjugaison par  $g$  induit un automorphisme (intérieur) de  $G$ , qui laisse donc  $D(G)$  invariant, ce qui revient à dire que  $G$  est distingué.

**Exercice 12.** (Conjugaison et transvections)

1. D'après l'exercice 6, toute transvection est donnée dans une base convenable par une même matrice. Comme les changements de bases sont donnés par des conjugaisons, on en déduit que toutes les transvections sont conjuguées dans  $\mathrm{GL}(E)$ .

2. On se place dans une base convenable, de sorte que  $v$  soit donnée par la matrice

$$\begin{pmatrix} I_{n-2} & 0 \\ 0 & T \end{pmatrix}$$

On considère  $s$  l'endomorphisme donné, dans la même base, par la matrice

$$\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & I_{n-1} \end{pmatrix}$$

Le déterminant de cette matrice est  $\lambda^{-1}$ , et comme  $n \geq 3$ , ces deux matrices commutent et  $sv = vs$ .

3. Soient  $u, v$  deux transvections. Il existe d'après la question 1 un élément  $g \in \text{GL}(E)$  tel que  $gug^{-1} = v$ . Soit  $\lambda = \det(g)$ , il existe d'après la question précédente un  $s \in \text{GL}(E)$  de déterminant  $\lambda^{-1}$  et qui commute avec  $u$ . On pose  $g' := gs \in \text{SL}(E)$ , et on a

$$g'ug'^{-1} = gsus^{-1}g^{-1} = gug^{-1} = v$$

soit le résultat voulu :  $g'$  est un élément de  $\text{SL}(E)$  qui conjugue  $u$  en  $v$ .

### Exercice 13.

1. Soient  $g, h \in \text{GL}(E)$ , on a

$$\det[g, h] = \det(g) \det(h) \det(g^{-1}) \det(h^{-1}) = 1$$

donc  $[g, h] \in \text{SL}(E)$ . Le groupe engendré par les commutateurs est donc un sous-groupe de  $\text{SL}(E)$ , soit le résultat voulu.

2. On sait que  $D(\text{GL}(E))$  est distingué dans  $\text{GL}(E)$ , donc  $D(\text{GL}(E))$  contient alors tous les conjugués de la transvection présente dans  $D(\text{GL}(E))$  par hypothèse. Comme toutes les transvections sont conjuguées dans  $\text{GL}(E)$ , on obtient que  $D(\text{GL}(E))$  contient en particulier toutes les transvections. Comme ces dernières engendrent  $\text{SL}(E)$ , on a  $\text{SL}(E) \subset D(\text{GL}(E))$  et  $\text{SL}(E) = D(\text{GL}(E))$  par la question précédente.

3.a) On sait que  $u = \tau(f, a)$  pour une certaine forme linéaire  $f$  et un vecteur  $a \in \ker(f)$ . On a vu que  $u^2 = \tau(f, 2a)$ . Comme  $\text{car}(k) \neq 2$ , on a  $2a \neq 0$  et  $\tau(f, 2a)$  est une transvection.

b) On sait que  $u$  et  $u^2$  sont conjugués dans  $\text{SL}(E)$  : il existe  $s \in \text{SL}(E)$  tel que  $sus^{-1} = u^2$ , on a donc  $sus^{-1}u^{-1} = u = [s, u]$ .

c) On a  $[s, u] = u \in \text{SL}(E)$  s'écrit comme un commutateur d'éléments de  $\text{SL}(E)$ , donc  $D(\text{SL}(E))$  contient une transvection, comme toutes les transvections sont conjuguées dans  $\text{SL}(E)$  (car  $n \geq 3$ ), on trouve  $D(\text{SL}(E)) = \text{SL}(E)$  et  $D(\text{GL}(E)) = \text{SL}(E)$ .

## 4 Action de $\text{GL}(E)$ sur l'espace projectif

### Exercice 14.

1. On sait que  $\text{GL}(E)$  est un sous-groupe du groupe  $\mathfrak{S}(E)$  des bijections de  $E$  dans lui-même. On trouve donc que  $\text{GL}(E)$  agit sur  $E$  par restriction de l'action de  $\mathfrak{S}(E)$ . Ensuite, pour  $u \in \text{GL}(E)$  et  $x \neq 0$ , on a  $u(x) \neq 0$ , donc l'action de  $\text{GL}(E)$  se restreint en une action sur  $E \setminus \{0\}$ .

Par définition, le morphisme structurel de l'action est l'inclusion  $\text{GL}(E) \subset \mathfrak{S}(E)$ , qui est injectif par définition. L'action est donc fidèle.

Soient  $x$  et  $y$  deux vecteurs non nuls. Si ils sont colinéaires, il existe une homothétie  $h \in \text{GL}(E)$  telle que  $h(x) = y$ . Si ils ne sont pas colinéaires, on peut les compléter en une base  $\{x, y, b_3, \dots, b_n\}$  de  $E$ , et considérer l'endomorphisme  $u$  défini par  $u(x) = y, u(y) = x, u(b_i) = b_i$ . Il s'agit bien d'un automorphisme ( $u^2 = \text{Id}_E$ ) qui envoie  $x$  sur  $y$ .

2. Si  $y = \lambda x$ , pour  $u \in \text{GL}(E)$  on a  $u(y) = \lambda u(x)$ , donc  $u(y)$  et  $u(x)$  sont colinéaires. L'action de  $\text{GL}(E)$  passe donc au quotient par  $u.D = u(D)$  pour  $D \in \mathbb{P}(E)$ .

3. Par définition, un élément  $u$  de  $\text{GL}(E)$  agit trivialement sur  $\mathbb{P}(E)$  si et seulement si il fixe globalement toutes les droites de  $E$ . On a vu à l'exercice 8 que cela implique que  $u$  est une homothétie. Et réciproquement, il est clair que les homothéties fixent globalement toutes les droites. Le noyau de l'action est donc donné par  $Z(\text{GL}(E))$ .

4. Le morphisme structurel de l'action de  $\text{GL}(E)$  se factorise d'après la question précédente en un morphisme injectif  $\text{PGL}(E) \rightarrow \mathfrak{S}(\mathbb{P}(E))$ , traduisant une action fidèle.

**Exercice 15.** ( $\text{PGL}_2(k)$  ou les homographies)

1. Commençons par noter que  $\psi$  est compatible avec l'action de  $k^*$  sur  $E \setminus \{0\}$  :

$$\forall \lambda \neq 0, \quad \psi(\lambda x, \lambda y) = \begin{cases} \frac{\lambda x}{\lambda y} = \frac{x}{y} & \text{si } \lambda y \neq 0 \Leftrightarrow y \neq 0 \\ \infty & \text{si } \lambda y = 0 \Leftrightarrow y = 0 \end{cases}$$

donc  $\psi$  induit une application  $\tilde{\psi}$  de  $\mathbb{P}^1(k)$  vers  $\widehat{k}$ , donnée par

$$\tilde{\psi}([x : y]) = \begin{cases} \frac{x}{y} & \text{si } y \neq 0, \\ \infty & \text{si } y = 0. \end{cases}$$

(on voit en particulier que l'information " $y = 0$ " ne dépend pas des coordonnées homogènes choisies).

On montre ensuite que  $\varphi$  et  $\tilde{\psi}$  sont des bijections réciproques l'une de l'autre. Soit  $[x : y] \in \mathbb{P}^1(k)$

- Si  $y = 0$ , on a

$$\varphi \tilde{\psi}([x : y]) = \varphi\left(\frac{x}{y}\right) = \left[\frac{x}{y} : 1\right] = \left[y \frac{x}{y} : y\right] = [x : y]$$

- Si  $y \neq 0$ , on a

$$\varphi(\tilde{\psi}([x : y])) = \varphi(\tilde{\psi}([x : 0])) = \varphi(\infty) = [1 : 0] = [x \cdot 1 : x \cdot 0] = [x : 0] = [x : y]$$

Donc  $\varphi \circ \tilde{\psi} = \text{Id}$ , on conclut de même pour  $\tilde{\psi} \circ \varphi$ .

2. On sait que l'action de  $u$  sur  $\mathbb{P}^1(k)$  est donnée par

$$u.[x : y] = [ax + by : cx + dy]$$

• Si  $c = 0$ , alors  $d \neq 0$  car  $u$  est inversible.

- Si  $x = \lambda \in k \subset \widehat{k}$ , on a

$$\varphi(u.\varphi^{-1}(x)) = \varphi(u.[\lambda, 1]) = \varphi([a\lambda + b : d]) = \frac{a\lambda + b}{d}$$

- Si  $x = \infty$ , alors

$$\varphi(u.\varphi^{-1}(x)) = \varphi(u.[1 : 0]) = \varphi([a : 0]) = \infty$$

Donc l'action de  $u$  est simplement une fonction affine sur  $k$ , étendue par  $u.\infty = \infty$ .

• Si  $c \neq 0$ , alors

- Si  $x = \frac{-d}{c}$ , on a

$$\varphi(u.\varphi^{-1}(x)) = \varphi(u.[-d : c]) = \varphi([-ad + bc : 0]) = \infty$$

- Si  $x \neq \frac{-d}{c}$  est un élément de  $k$ , on a

$$\varphi(u.\varphi^{-1}(x)) = \varphi(u.[x : 1]) = \varphi([ax + b : cx + d]) = \frac{ax + b}{cx + d}$$

- Si  $x = \infty$ , on a

$$\varphi(u.\varphi^{-1}(x)) = \varphi(u.[1 : 0]) = \varphi([a : c]) = \frac{a}{c}$$

Au total, on retrouve que  $u$  est donnée par les homographies au sens classique

$$x \mapsto \frac{ax + b}{cx + d}$$

étendue par  $u(\infty) = \frac{a}{c}$  et  $u(\frac{-d}{c}) = \infty$ , avec la convention  $\frac{1}{\infty} = 0$ .

3. D'après l'exercice 10,  $\text{PSL}(E)$  vu comme un sous-groupe de  $\text{PGL}(E)$  est le noyau de l'application  $\overline{\det}$ . On a donc  $u \in \text{PSL}_2(k)$  si et seulement si  $\det(u)$  est un carré dans  $k^*$ .

**Exercice 16.** (Isomorphismes exceptionnels)

1. On sait que  $\mathbb{F}_q^*$  agit fidèlement et transitivement sur  $\mathbb{F}_q^{n+1} \setminus \{0\}$ , on en conclut donc que

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^{n+1}| - 1}{|\mathbb{F}_q^*|} = \frac{q^{n+1} - 1}{q - 1} = 1 + q + \dots + q^n$$

2. C'est le morphisme structurel de l'action de  $\mathrm{PGL}_2(\mathbb{F}_q)$  sur  $\mathbb{P}^1(k)$ . Il est injectif car l'action est fidèle par l'exercice précédent.

3. Comme  $k^* = \{1\}$ , on a  $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2)$  est un groupe d'ordre 6. Comme on a un morphisme injectif  $\mathrm{PGL}_2(\mathbb{F}_2) \rightarrow \mathfrak{S}_3$ , on conclut que ces groupes sont égaux à  $\mathfrak{S}_3$ . Le groupe dérivé de  $\mathfrak{S}_3$  est d'ordre 3 (c'est le groupe engendré par les trois cycles), le groupe associé dans  $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2)$  est engendré par la matrice

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

4. On sait que  $\mathrm{PGL}_2(\mathbb{F}_3)$  et  $\mathrm{PSL}_2(\mathbb{F}_3)$  sont respectivement d'ordre 24 et 14. Le morphisme injectif  $\mathrm{PGL}_2(\mathbb{F}_3) \rightarrow \mathfrak{S}_4$  donne donc  $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ . Comme  $\mathrm{PSL}_2(\mathbb{F}_3)$  est un sous-groupe d'indice 2 de  $\mathrm{PGL}_2(\mathbb{F}_3)$ , et que  $\mathfrak{A}_4$  est l'unique sous-groupe d'indice 2 de  $\mathfrak{S}_4$ , on conclut que  $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$ .

Le groupe dérivé de  $\mathfrak{A}_4$  est un groupe d'ordre 4 engendré par les doubles transpositions. Ensuite, comme le morphisme  $\mathrm{SL}_2(\mathbb{F}_3) \rightarrow \mathrm{PSL}_2(\mathbb{F}_3)$  est surjectif, il induit une surjection des commutateurs de  $\mathrm{SL}_2(\mathbb{F}_3)$  vers ceux de  $\mathrm{PSL}_2(\mathbb{F}_3)$ , d'où un morphisme surjectif  $D(\mathrm{SL}_2(\mathbb{F}_3)) \rightarrow D(\mathrm{PSL}_2(\mathbb{F}_3))$ , et même  $D(\mathrm{SL}_2(\mathbb{F}_3))$  est l'image réciproque de  $D(\mathrm{PSL}_2(\mathbb{F}_3))$  par la projection, donc  $D(\mathrm{SL}_2(\mathbb{F}_3))$  est d'ordre 8, et il admet  $Z(\mathrm{SL}_2(\mathbb{F}_3))$  comme sous-groupe distingué, d'ordre 2. D'où  $D(\mathrm{SL}_2(\mathbb{F}_3)) \simeq Q_8$  le groupe des quaternions.

5. À nouveau grâce aux cardinaux, on a  $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4)$  est d'indice 2 dans  $\mathfrak{S}_5$ , il s'agit donc du groupe alterné  $\mathfrak{A}_5$ .

6. On a un morphisme injectif  $\mathrm{PGL}_2(\mathbb{F}_5) \rightarrow \mathfrak{S}_6$ , dont l'image est d'indice  $n$ , d'où  $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ , et  $\mathrm{PSL}_2(\mathbb{F}_5)$  est d'indice 2 dans  $\mathrm{PGL}_2(\mathbb{F}_5)$ , d'où  $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$ .

## 5 Quelques sous-groupes finis de $\mathrm{GL}_n(k)$

**Exercice 17.**

1. Il est clair que  $u_\sigma$  est bien un automorphisme de  $k^n$  (car permuter une base est bien une opération inversible). Ensuite, on a, pour  $\sigma, \tau \in \mathfrak{S}_n$  :

$$\sigma.\tau.e_i = \sigma.e_{\tau(i)} = e_{\sigma(\tau(i))} = (\sigma\tau).e_i$$

donc  $u_{\sigma\tau} = u_\sigma u_\tau$  sur la base canonique, ce qui s'étend à  $k^n$  par linéarité.

2. Le morphisme  $\mathfrak{S}_n \rightarrow \mathrm{GL}_n(k)$  est simplement le morphisme structurel de l'action précédente (action par permutation sur une base).

3. Soit  $\tau = (i \ j)$  une transposition, l'action de  $\tau$  est donnée par

$$\tau.e_k = \begin{cases} e_k & \text{si } k \notin \{i, j\} \\ e_j & \text{si } k = i \\ e_i & \text{si } k = j \end{cases}$$

Donc la matrice de  $\tau$  est  $I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$ . Par exemple pour  $n = 3$

$$P_{(1 \ 3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad P_{(1 \ 2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



4. Soit  $\sigma$  tel que  $P_\sigma = I_n$ , où de manière équivalente,  $u_\sigma = \text{Id}$ . Pour tout  $i \in \llbracket 1, n \rrbracket$ , on a  $u_\sigma(e_i) = e_i = e_{\sigma(i)}$ , donc  $\sigma(i) = i$ . Donc  $\sigma = 1$ , et l'application considérée est injective (i.e l'action par permutation est une action fidèle).

5. Soit  $\rho \in \mathfrak{S}_n$  une permutation telle que  $\rho\sigma\rho^{-1} = \tau$ . Comme  $\sigma \mapsto P_\sigma$  est un morphisme de groupes, on a  $P_\rho P_\sigma P_\rho^{-1} = P_\tau$  d'où le résultat.

6. On sait que le déterminant est une forme  $n$ -linéaire alternée. Or la matrice de la transposition  $(i\ j)$  est obtenue à partir de  $I_n$  en permutant la  $i$ -ème et la  $j$ -ème colonne. D'où  $\det(P_{(i\ j)}) = -1$ .

On sait que les transpositions engendrent  $\mathfrak{S}_n$ , et que  $\sigma \mapsto \det(P_\sigma)$  est un morphisme de groupe, qui coïncide avec la signature sur les transpositions, on obtient  $\varepsilon(\sigma) = \det(P_\sigma)$  pour toute transposition  $\sigma$ .

### Exercice 18.

1. Soient  $a, b \in G$ , on a  $(ab)^2 = abab = 1$ , de même  $1 = a^2b^2 = aabb$ . En simplifiant par  $a$  à gauche et  $b$  à droite, il vient  $ab = ba$ . Ainsi,  $G$  est abélien car tous ses éléments commutent.

2. Soit  $M \in G$  non triviale. Par hypothèse, on a  $M^2 = I_n$ , donc  $M$  est racine du polynôme  $X^2 - 1 = (X - 1)(X + 1)$ . Comme nous sommes en caractéristique non 2, ce polynôme est scindé à racines simples, donc  $M$  est diagonalisable, avec uniquement des  $\pm 1$  sur la diagonale. D'après la question précédente, le groupe  $G$  est abélien. Par le théorème de diagonalisation simultanée, il existe  $P \in \text{GL}_n(k)$  telle que  $PGP^{-1}$  soit constitué de matrices diagonales avec des  $\pm 1$  sur la diagonale. On sait qu'il y a  $2^n$  telles matrices, donc  $|G| = |PGP^{-1}| \leq 2^n$ .

3. Considérons le sous-groupe  $G$  de  $\text{GL}_n(k)$  formé des matrices diagonales avec des  $\pm 1$  sur la diagonale. C'est un sous-groupe de  $\text{GL}_n(k)$  d'exposant 2 et de cardinal  $2^n$ . Si l'on a un morphisme injectif  $\text{GL}_n(k) \rightarrow \text{GL}_m(L)$ , alors l'image de  $G$  par ce morphisme est un sous-groupe d'exposant 2 de  $\text{GL}_m(L)$  et de cardinal  $2^n$ . Par la question précédente, on obtient  $2^n \leq 2^m$  et  $n \leq m$ .

4. Par la question précédente, l'existence d'un isomorphisme  $\text{GL}_n(k) \simeq \text{GL}_m(L)$  force  $m \leq n$  et  $n \leq m$ .

5. Comme  $\mathbb{Q}$  est dénombrable, il en va de même de  $\text{GL}_n(\mathbb{Q}) \approx \mathbb{Q}^{n^2}$ . Ce groupe ne peut être isomorphe à  $\text{GL}_m(\mathbb{R})$ , qui est indénombrable (son centre, isomorphe à  $\mathbb{R}^*$ , est indénombrable). Ensuite, on sait que  $\mathbb{R}^*$  et  $\mathbb{C}^*$  ne sont pas isomorphes (le second contient des éléments d'ordre 3, contrairement au premier). Comme ce sont les centres respectifs de  $\text{GL}_n(\mathbb{R})$  et  $\text{GL}_m(\mathbb{C})$ , ces deux groupes ne peuvent être isomorphes.

### Exercice 19. (Ceci n'est pas un exercice sur les représentations)

1. On sait par le théorème de Cayley que tout groupe d'ordre  $n$  admet un morphisme injectif vers  $\mathfrak{S}_n$ . On sait par ailleurs qu'il existe un morphisme injectif  $\mathfrak{S}_n \rightarrow \text{GL}_n(k)$ . On obtient le résultat par composition.

2. Il faut commencer par décrire le morphisme  $D_4 \rightarrow \mathfrak{S}_8$ . On rappelle que  $D_4$  est donné par la présentation suivante

$$D_4 = \langle r, s \mid s^2 = 1, r^4 = 1, srs = r^{-1} \rangle$$

Sous cette présentation, les éléments de  $D_4$  sont les suivants

$$D_4 = \left\{ \begin{array}{cccc} 1 & r & r^2 & r^3 \\ s & sr & sr^2 & sr^3 \end{array} \right\}$$

On numérote ces éléments de la façon suivante :  $1 \rightarrow 1, r \rightarrow 2, \dots, s \rightarrow 5, \dots, sr^3 \rightarrow 8$ . En faisant le produit par  $s$  à gauche, on obtient

$$sD_4 = \left\{ \begin{array}{cccc} s & sr & sr^2 & sr^3 \\ 1 & r & r^2 & r^3 \end{array} \right\}$$

Donc le produit par  $s$  induit la permutation  $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$ . De même pour le produit par  $r$  (en utilisant  $rsr^i = sr^{i-1}$ )

$$rD_4 = \left\{ \begin{array}{cccc} r & r^2 & r^3 & 1 \\ sr^3 & s & sr & sr^2 \end{array} \right\}$$

Donc le produit par  $r$  induit la permutation  $(1\ 2\ 3\ 4)(5\ 8\ 7\ 6)$ . Les matrices associées respectivement à  $s$  et  $r$  sont alors

$$P_r = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \quad \text{et} \quad P_s := \begin{pmatrix} 0 & I_4 \\ I_4 & 0 \end{pmatrix}$$

avec

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

On déduit les valeurs des autres matrices par le produit de  $s$  et de  $r$ .

**Exercice 20.** (Un groupe de réflexions)

1. Soit  $P_\sigma$  une matrice de permutation, par définition la  $i$ -ème colonne de  $P_\sigma$  est donnée par les coordonnées du vecteur  $e_{\sigma(i)}$ , qui contient donc un unique coefficient non nul. De même la  $i$ -ème ligne est le vecteur  $e_{\sigma^{-1}(i)}$  (car  ${}^t P_\sigma = P_{\sigma^{-1}}$ ).

2. Soit  $M \in G(m, 1, n)$ , on pose  $\lambda_i$  l'unique coefficient non nul de la  $i$ -ème colonne de  $M$ . Pour  $i \in \llbracket 1, n \rrbracket$ , il existe un unique  $j \in \llbracket 1, n \rrbracket$  tel que  $M.e_i = \lambda_i e_j$ . La correspondance  $i \mapsto j$  est une bijection  $\sigma$  (car il existe un unique coefficient non nul sur chaque ligne). En posant  $D = \text{diag}(\lambda_i)$  on obtient que  $M = P_\sigma D$  est sous la forme voulue.

Pour l'unicité, la matrice  $P_\sigma D$  est définie par  $(P_\sigma D).e_i = D.e_{\sigma(i)}$ , ce qui caractérise complètement  $P_\sigma D$ .

3. Soit  $i \in \llbracket 1, n \rrbracket$ , on a

$$P_\sigma^{-1} D P_\sigma(e_i) = P_\sigma^{-1} D.e_{\sigma(i)} = P_\sigma^{-1} D_{\sigma(i)} e_{\sigma(i)} = D_{\sigma(i)} e_i$$

Donc  $P_\sigma^{-1} D P_\sigma$  est une matrice diagonale, dont le  $i$ -ème coefficient diagonal est  $D_{\sigma(i)}$ . On note  $D^\sigma$  cette matrice.

Soit  $P_\sigma D \in G(m, 1, n)$ , on a  $(P_\sigma D)^{-1} = D^{-1} P_{\sigma^{-1}} = P_{\sigma^{-1}} (D^{-1})^{\sigma^{-1}} \in G(m, 1, n)$  car  $\mu_m(k)$  est stable par inverse (donc  $D^{-1}$  et  $(D^{-1})^{\sigma^{-1}}$  sont bien à coefficients dans  $\mu_m(k)$ ).

Soient  $P_\sigma D$  et  $P_\tau \Delta$  deux éléments de  $G(m, 1, n)$ , on a

$$P_\sigma D P_\tau \Delta = P_\sigma P_\tau D^\sigma \Delta = P_{\sigma\tau} D^\sigma \Delta \in G(m, 1, n)$$

donc ce dernier est bien un sous-groupe de  $\text{GL}_n(k)$  (en fait un produit semi-direct de  $\mu_m(k)^n$  par  $\mathfrak{S}_n$ ).

4. Si  $M = P_\sigma D$ , le produit des coefficients non nuls de  $M$  est  $\det(D)$ , or on a

$$P_\sigma D P_\tau \Delta = P_{\sigma\tau} D^\tau \Delta$$

et  $\det(D) \det(\Delta) = \det(D^\tau) \det(\Delta) = \det(D^\tau \Delta)$ , on a donc bien affaire à un morphisme de groupes.

5. Pour  $G(m, 1, 2)$ , on doit choisir un élément de  $\mathfrak{S}_2$ , et deux coefficients dans  $\mu_m(\mathbb{C})$ , donc  $2m^2$  choix possibles. Comme le morphisme donnant le produit des coefficients est surjectif à valeurs dans  $\mu_m(\mathbb{C})$ , son noyau est de cardinal  $\frac{2m^2}{m} = 2m$ , d'où le résultat.

6. Les relations matricielles sont évidentes. Soit ensuite une matrice  $M \in G(m, m, 2)$  on a

$$M = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \quad \text{ou} \quad M = \begin{pmatrix} 0 & \zeta^{-1} \\ \zeta & 0 \end{pmatrix}$$

pour un certain  $\zeta \in \mu_m(2)$ . On pose  $\zeta = \zeta_m^k$ , dans le premier cas, on a  $M r^{-k} = I_2$  et dans le second  $M r^k = s$ . Donc  $r$  et  $s$  engendrent bien  $G(m, m, 2)$ .

7. Le fait que  $s$  et  $r$  respectent les relations de la présentation de  $D_m$  donne un morphisme surjectif  $D_m \twoheadrightarrow \langle r, s \rangle$ . Mais ce dernier groupe est égal à  $G(m, m, 2)$ , d'ordre  $2m$ , d'où l'égalité.