Groupe linéaire : correction

Exercice 1. Une matrice $\mathrm{M} = (m_{i,j})_{i,j}$ appartenant au centre de $\mathrm{M}_n(\mathrm{A})$ doit au moins commuter avec les matrices élémentaires $e_{j,k}$. Or,

$$\mathrm{M}e_{k,l} = \left(\sum_{i,j} m_{i,j}e_{i,j}\right) e_{k,l} = \sum_i m_{i,k}e_{i,l} \qquad e_{k,l}\mathrm{M} = e_{k,l}\left(\sum_{i,j} m_{i,j}e_{i,j}\right) = \sum_j m_{l,j}e_{k,j}.$$

Ainsi, si M commute avec $e_{j,k}$, on doit avoir

$$\forall i \neq k, m_{i,k} = 0 \qquad \forall j \neq k, m_{l,j} = 0 \qquad m_{k,k} = m_{l,l}.$$

Une matrice $\mathrm{M} \in \mathrm{Z}(\mathrm{M}_n(\mathrm{A}))$ est donc forcément scalaire : il existe $\lambda \in \mathrm{A}$ tel que $\mathrm{M} = \lambda \mathrm{I}_n$. Comme cette matrice doit également commuter avec tous les $\mu\mathrm{I}_n$, $\mu \in \mathrm{A}$, il vient $\lambda \in \mathrm{Z}(\mathrm{A})$. La réciroque étant évidente, on a bien

$$\mathrm{Z}(\mathrm{M}_n(\mathrm{A})) = \left\{ \lambda \mathrm{I}_n \,\middle|\, \lambda \in \mathrm{Z}(\mathrm{A}) \right\}.$$

Exercice 2. Une matrice $\mathrm{M} \in \mathrm{M}_n(\mathbf{F}_q)$ est inversible si et seulement si les vecteurs colonnes forment une base. Il suffit pour cela que le premier vecteur soit non nul, que le deuxième ne soit pas colinéaire au premier, que le troisième n'appartienne pas au plan engendré par les deux premiers, etc. On obtient donc

$$|\mathrm{GL}_n(\mathbf{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1)\cdots(q - 1).$$

$\mathrm{SL}_n(\mathbf{F}_q)$ est le noyau du morphisme surjectif $\mathrm{GL}_n(\mathbf{F}_q) \to \mathbf{F}_q^*$. Puisque $|\mathbf{F}_q^*| = q - 1$, on a

$$|\mathrm{SL}_n(\mathbf{F}_q)| = \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{q-1} = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1)\cdots(q^2 - 1).$$

$\mathrm{PGL}_n(\mathbf{F}_q)$ est le quotient de $\mathrm{GL}_n(\mathbf{F}_q)$ par son centre. D'après le cours, celui-ci est constitué des matrices scalaires $\lambda\mathrm{I}_n$ ($\lambda \in \mathbf{F}_q^*$), qui forment un ensemble de cardinal $q - 1$. On obtient donc le même cardinal

$$|\mathrm{PGL}_n(\mathbf{F}_q)| = \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{q-1} = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1)\cdots(q^2 - 1).$$

Il est également vrai que les matrices de $\mathrm{SL}_n(\mathbf{F}_q)$ sont centrales si et seulement si elles sont scalaires (une matrice dans le centre de $\mathrm{SL}_n(\mathbf{F}_q)$ soit commuter avec toutes les matrices de transvection $1 + e_{i,j}$ ($i \neq j$), ce qui revient à commuter avec les matrices $e_{i,j}$; le début de la preuve de l'exercice 1 entraîne alors que la matrice est scalaire). Les matrices scalaires de $\mathrm{SL}_n(\mathbf{F}_q)$ sont les $\lambda\mathrm{I}_n$, avec λ racine n-ième de l'unité. Il s'agit donc maintenant de dénombrer $\mu_n(\mathbf{F}_q)$. Nous allons montrer que son cardinal est $d = \mathrm{pgcd}(n, q-1)$ (c'est en fait un résultat général : il y a $\mathrm{pgcd}(r, s)$ éléments d'ordre divisant r dans un groupe cyclique d'ordre s).
En effet, soit u et v tels que $d = u(q-1) + vn$. Si $x \in \mu_n(\mathbf{F}_q)$, alors $x^n = 1$, et donc $x^d = (x^n)^v(x^{q-1})^u = 1$. Inversement, si $x^d = 1$, alors $x^n = 1$. Donc on a égalité entre $\mu_n(\mathbf{F}_q)$

et $\mu_d(\mathbf{F}_q)$. Mais le polynôme $X^{q-1}-1$ est déjà scindé et à racines simples sur $\mathbf{F}_q$, donc on peut en dire autant de X^d-1 qui en est un diviseur. Bref, $|\mu_n(\mathbf{F}_q)| = |\mu_d(\mathbf{F}_q)| = d$.
On a donc

$$|\mathrm{PSL}_n(\mathbf{F}_q)| = \left|\frac{\mathrm{PSL}_n(\mathbf{F}_q)}{\mathrm{Z}(\mathrm{PSL}_n(\mathbf{F}_q))}\right| = \frac{|\mathrm{SL}_n(\mathbf{F}_q)|}{\mathrm{pgcd}(q-1,n)} = q^{n(n-1)/2}\frac{(q^n-1)(q^{n-1}-1)\cdots(q^2-1)}{\mathrm{pgcd}(q-1,n)}.$$

Exercice 3. Soit G un sous-groupe distingué de $\mathrm{SL}_n(\mathrm{K})$, distinct de $\mathrm{SL}_n(\mathrm{K})$. On peut considérer l'application canonique $\varphi : \mathrm{SL}_n(\mathrm{K}) \longrightarrow \mathrm{PSL}_n(\mathrm{K})$ qui est surjective, donc $\varphi(\mathrm{G})$ est distingué dans $\mathrm{PSL}_n(\mathrm{K})$. Puisque $\mathrm{PSL}_n(\mathrm{K})$ est simple, c'est donc que $\varphi(\mathrm{G})$ est trivial ou est $\mathrm{PSL}_n(\mathrm{K})$ tout entier. Montrons que ce dernier cas ne peut pas se produire. Si $\varphi(\mathrm{G}) = \mathrm{PSL}_n(\mathrm{K})$, alors G contient un antécédent de $\left[\begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}\right]$, qui est nécessairement de la forme $\lambda \begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$ avec $\lambda \in \mu_n(\mathrm{K})$. Élevons alors cette matrice à la puissance $d = \mathrm{pgcd}(n, q-1)$, ce qui donne $\begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & d \\ & & & 1 \end{pmatrix}$. Ce dernier élément est une transvection (car $d \neq 0$ dans K), et puisque toutes les transvections sont conjuguées dans $\mathrm{SL}_n(\mathrm{K})$ et que G est distingué, c'est que G contient toutes les transvections. Or, les transvections engendrent $\mathrm{SL}_n(\mathrm{K})$, donc $\mathrm{G} = \mathrm{SL}_n(\mathrm{K})$. Ainsi, $\varphi(\mathrm{G})$ est réduit à l'élément neutre, et donc G est inclus dans le centre de $\mathrm{SL}_n(\mathrm{K})$, et donc de la forme $\{\lambda \mathrm{I}_n, \lambda \in \mathrm{T}\}$, où T est un sous-groupe de racines de l'unité de K^*. Or, on sait que pour un corps fini, K^* est cyclique, de même que tous ses sous-groupes.

Exercice 4.

1. Soit $\mathscr{B}$ une base, et soit G le sous-groupe de $\mathrm{GL}_n(\mathbf{F}_q)$ formé des g tels que la matrice de g dans $\mathscr{B}$ soit triangulaire supérieure, avec des 1 sur la diagonale. Comme il existe $\frac{n(n-1)}{2}$ coefficients au dessus de la diagonale, G est un groupe de cardinal $q^{\frac{n(n-1)}{2}}$. Or, on sait que le cardinal de $\mathrm{GL}_n(\mathbf{F}_q)$ est $(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$, ses p-sous-groupes de Sylow doivent être de cardinal $q^{\frac{n(n-1)}{2}}$. Donc G est justement un p-sous-groupe de Sylow. Comme ils sont de plus tous conjugués, leurs éléments ont tous pour polynôme caractéristique $(X-1)^n$, et tous peuvent être trigonalisés dans une même base.
2. Dans la question précédente, on a vu qu'il était possible de construire un p-sous-groupe de Sylow uniquement grâce à la donnée d'une base, mais il est possible que deux bases différentes donnent le même p-sous-groupe de Sylow : par exemple, si un endomorphisme a une matrice triangulaire supérieure (dans toute la suite, *triangulaire* voudra dire *triangulaire supérieure*) dans la base (e_1, e_2), il l'est également dans la base $(2e_1, 3e_2)$ ou dans la base (e_1, e_2+e_1). On va voir que la notion de drapeau est plus adaptée à la situation.

   Une base $\mathscr{B} = (e_1, \ldots, e_n)$ définit un drapeau complet $\mathbf{F}(\mathscr{B}) = (\mathrm{F}_i)_{i=0}^n$ tel que $\mathrm{F}_i = \mathrm{Vect}(e_1, \ldots, e_n)$. Un endomorphisme est alors triangulaire dans la base $\mathscr{B}$ s'il stabilise le drapeau $\mathbf{F}(\mathscr{B})$, c'est-à-dire si $\forall i \in [\![1, n]\!], u(\mathrm{F}_i) \subset \mathrm{F}_i$. On voit facilement que tout

drapeau complet est de la forme $\mathbf{F}(\mathscr{B})$ pour une certaine base $\mathscr{B}$ (mais qui est loin d'être unique, comme on l'a vu).

En résumé, toute base $\mathscr{B} = (e_1, \dots, e_n)$ définit un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$ qui ne dépend d'ailleurs que du drapeau $\mathbf{F}(\mathscr{B})$. Comme on a vu que tout p-sous-groupe de Sylow est obtenu de cette matière, on a bien défini une application surjective, où l'on a noté $\mathscr{D}(\mathbf{F}_q^n)$ l'ensemble des drapeaux complets de $\mathbf{F}_q^n$:

$$\Phi : \begin{array}{ccc} \mathscr{D}(\mathbf{F}_q^n) & \to & \mathrm{Syl}_p(\mathrm{GL}_n(\mathbf{F}_q)) \\ \mathbf{F} & \mapsto & \left\{ u \in \mathrm{GL}_n(\mathbf{F}_q) \,\middle|\, \chi_u(\mathrm{X}) = (\mathrm{X}-1)^n \text{ et } u \text{ stabilise } \mathbf{F} \right\}. \end{array}$$

Il reste maintenant à montrer que cette application est injective, c'est-à-dire qu'un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$ ne stabilise qu'un seul drapeau complet.

En fait, nous allons démontrer un résultat plus fort, à savoir que l'endomorphisme u représenté dans une certaine base $\mathscr{B}$ par la matrice de Jordan

$$\mathrm{J}_n(1) = \begin{pmatrix} 1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix}$$

ne stabilise déjà que le drapeau $\mathbf{F}(\mathscr{B})$. Nous allons même donner deux preuves de ce fait.

Première preuve : on procède par récurrence.

Le cas $n = 1$ est tautologique (l'ensemble $\mathscr{D}(\mathbf{F}_q)$ est réduit au singleton $\{(0, \mathbf{F}_q)\}$). Analysons toutefois le cas $n = 2$, qui nous fournira l'argument-clef. En dimension 2, la donnée d'un drapeau complet $\mathbf{F}$ se réduit à celle de la droite F_1. Il s'agit donc de déterminer les droites stables (c'est-à-dire propres) de u.

Or, même en dimension n, u est de spectre $\{1\}$, donc 1 est la seule valeur propre. Comme en outre, $\mathrm{rg}(u - \mathrm{id}) = n - 1$, l'espace propre $\ker(u - \mathrm{id})$ est de dimension 1 et il n'y a donc qu'une droite propre, engendrée par le premier vecteur e_1 de la base $\mathscr{B}$.

Supposons donc maintenant le résultat démontré en dimension $n - 1$ et soit u un endomorphisme u représenté dans une certaine base $\mathscr{B} = (e_1, \dots, e_n)$ par $\mathrm{J}_n(1)$. Soit $\mathbf{F} = (\mathrm{F}_0 = \{0\}, \mathrm{F}_1, \dots, \mathrm{F}_n = \mathbf{F}_q^n)$ un drapeau stabilisé par u. D'après ce qui précède, la droite F_1 est nécessairement $\mathrm{Vect}(e_1)$. Le drapeau $\mathbf{F}$ est donc déterminé par un choix de supplémentaire à F_1 dans chacun des F_i, pour $i \geq 2$, voire, plus intrinsèquement, par les images $\overline{\mathrm{F}}_i = \mathrm{F}_i/\mathrm{F}_1$ des F_i dans l'espace vectoriel quotient $\overline{\mathrm{E}} = (\mathbf{F}_q^n)/\mathrm{F}_1$.

La condition que $\mathbf{F}$ soit stabilisé par u est alors équivalente à celle que le drapeau $\overline{\mathbf{F}} = (\overline{\mathrm{F}}_i)_{i=1}^n$ soit stabilisé par l'endomorphisme $\overline{u}$ de $\overline{\mathrm{E}}$ induit par u. Observons que la famille $\overline{\mathscr{B}} = (\overline{e_2}, \dots, \overline{e_n})$ (où $\overline{e_i}$ est l'image de e_i par la projection $\mathbf{F}_q^n \to \overline{\mathrm{E}}$) est une base de $\overline{\mathrm{E}}$. Puisqu'on avait initialement $u(e_1) = e_1$ et, pour $i \geq 2$, $u(e_i) = e_i + e_{i-1}$, on a dans $\overline{\mathrm{E}}$ les égalités $u(\overline{e_2}) = \overline{e_2 + e_1} = \overline{e_2}$ et, pour $i \geq 3$, $u(\overline{e_i}) = \overline{e_i} + \overline{e_{i-1}}$, c'est-à-dire que $\mathrm{Mat}_{\overline{\mathscr{B}}} \overline{u} = \mathrm{J}_{n-1}(1)$.

D'après l'hypothèse de récurrence, $\mathbf{F}(\overline{\mathscr{B}})$ est le seul drapeau stabilisé par $\overline{u}$, et $\mathbf{F}(\mathscr{B})$ est donc le seul drapeau stabilisé par u.

Remarque. Il est sans aucun doute possible d'écrire cette preuve à coups de supplémentaires pour éviter l'utilisation de la notion d'espace vectoriel quotient. Le lecteur pourra se livrer à cette traduction, mais la notion de quotient semble ici particulièrement pertinente, et il vaut sans doute mieux se familiariser avec son utilisation.

Deuxième preuve : on va utiliser le formalisme des K[X]-modules (ici, $\mathrm{K} = \mathbf{F}_q$). Nous allons en fait démontrer le même résultat que précédemment pour un endomorphisme u représenté dans une certaine base par la matrice de Jordan

$$\mathrm{J}_n(0) = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}.$$

Les deux résultats sont clairement équivalents (un espace est stable par u si et seulement s'il l'est par $u \pm \mathrm{id}$), mais cela simplifiera quelque peu les notations.

Comme expliqué en algèbre 1, la donnée d'un K[X]-module E est exactement la même chose que celle d'un K-espace vectoriel (= K-module) E et d'un endomorphisme $u : \mathrm{E} \to \mathrm{E}$ (qui joue le rôle de la multiplication par X). En outre, deux endomorphismes semblables fournissent des K[X]-modules isomorphes. Étant donné un K-espace vectoriel E et un endomorphisme $u : \mathrm{E} \to \mathrm{E}$, on pourra noter E_u le K[X]-module correspondant.

Le bloc de Jordan $\mathrm{J}_n(0)$ correspond alors au K[X]-module $\mathrm{K}[\mathrm{X}]/(\mathrm{X}^n)$. Ce module est en effet un K-espace vectoriel de dimension n, dont une base est par exemple $\mathscr{B} = (\mathrm{X}^{n-1}, \dots, \mathrm{X}, 1)$ et il est immédiat de constater que la matrice de la multiplication par X dans cette base est $\mathrm{J}_n(0)$.

En général, à quoi correspond dans ce langage un sous-espace stable ? Un sous-espace u-stable de E est un sous-K-espace vectoriel $\mathrm{F} \subset \mathrm{E}$ tel que $u(\mathrm{F}) \subset \mathrm{F}$. Il doit donc correspondre à un sous-K-espace vectoriel de E_u invariant par multiplication par X, c'est-à-dire un sous-K[X]-module de E_u. C'est un principe général, dans le langage des K[X]-modules, *un sous-espace stable correspond à un sous-*K[X]*-module !*

Nous sommes donc amenés à étudier les sous-K[X]-modules du module $\mathrm{M} = \mathrm{K}[\mathrm{X}]/(\mathrm{X}^n)$ et plus précisément à déterminer qu'il n'y a que les sous-K[X]-modules correspondant au drapeau $\mathbf{F}(\mathscr{B})$, à savoir les $\mathrm{M}_k = (\mathrm{X}^k\mathrm{K}[\mathrm{X}])/(\mathrm{X}^n)$ pour $k \in [\![0, n]\!]$. (Notons que vu la base $\mathscr{B}$, M_k correspond à $\mathrm{Vect}(e_1, \dots, e_{n-k})$).

Mais un peu d'algèbre rend cette tâche facile : le K[X]-module M est le quotient du K[X]-module K[X] par son K[X]-sous-module (X^n) (souvenons-nous : un sous-A-module du A-module A n'est rien d'autre qu'un idéal.) Il y a donc un couple de bijections induites par la surjection $\pi : \mathrm{K}[\mathrm{X}] \to \mathrm{M}$:

$$\begin{array}{rccc} & \{\text{sous-module N} \subset \mathrm{M}\} & \leftrightarrow & \{\text{sous-module } (\mathrm{X}^n) \subset \mathrm{P} \subset \mathrm{K}[\mathrm{X}]\}. \\ \pi^* : & \mathrm{N} & \mapsto & \pi^{-1}[\mathrm{N}] \\ & \pi[\mathrm{P}] & \hookleftarrow & \mathrm{P} \qquad\qquad : \pi_* \end{array}$$

Or, K[X] est un anneau principal : les sous-K[X]-modules de K[X] (= idéaux) sont donc exactement les PK[X], pour P unitaire (ou nul). Ceux qui contiennent l'idéal (X^n) sont donc les $\mathrm{X}^k\mathrm{K}[\mathrm{X}]$ pour $k \in [\![0, n]\!]$ (il faut que P divise X^n) et leurs images par π_* sont bien les M_k.

Remarques.

– On a en fait démontré un résultat plus fort, à savoir que les éléments du drapeau $\mathbf{F}(\mathscr{B})$ sont les seuls sous-espaces vectoriels de $\mathbf{F}_q^n$ stables par u. Il serait relativement aisé de modifier la première preuve pour qu'elle démontre ce résultat-ci.

– Passer de $\mathrm{J}_n(1)$ à $\mathrm{J}_n(0)$ nous a essentiellement permis de travailler avec le module $\mathrm{K}[\mathrm{X}]/(\mathrm{X}^n)$ et sa K-base $(1, \mathrm{X}, \dots, \mathrm{X}^{n-1})$ partout où il aurait sinon fallu avoir $\mathrm{K}[\mathrm{X}]/((\mathrm{X}-1)^n)$ et $(1, \mathrm{X}-1, \dots, (\mathrm{X}-1)^{n-1})$. Il n'y a eu aucune simplification conceptuelle. Le lecteur est invité à s'en convaincre.

– Chacune des deux preuves n'utilise aucunement le fait que le corps de base soit ici fini. Les résultats tiennent donc dans n'importe quel corps.

On a donc obtenu une bijection Φ entre l'ensemble $\mathscr{D}(\mathbf{F}_q^n)$ des drapeaux complets de $\mathbf{F}_q^n$ et l'ensemble des p-sous-groupes de Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$. Il reste à dénombrer $\mathscr{D}(\mathbf{F}_q^n)$. Le cardinal de l'ensemble des hyperplans de $\mathbf{F}_q^n$ est $(q^n-1)/(q-1) = 1+q+\cdots+q^{n-1}$ (c'est le nombre de formes linéaires non nulles, à homothétie près), et par définition, un drapeau complet est une suite de sous-espaces (E_i) tels que E_{i-1} soit un hyperplan de E_i. L'ensemble des drapeaux complets, et donc celui des p-sous-groupes de Sylow de $\mathrm{GL}_n(\mathbf{F}_q)$ est donc de cardinal

$$\frac{(q^n-1)\dots(q-1)}{(q-1)^n} = \prod_{k=1}^{n}(1+q+\cdots+q^{k-1}).$$

On remarque facilement et avec soulagement que ce nombre est bien congru à 1 modulo p et qu'il divise $|\mathrm{GL}_n(\mathbf{F}_q)|/p^{n(n-1)/2} = (q^n-1)(q^{n-1}-1)\cdots(q-1)$.

Exercice 5. Le résultat est très classique dans le cas où $r=1$: une application linéaire qui laisse stable toutes les droites est une homothétie, nous allons essayer de nous y ramener. Soit donc D une droite de E, montrons que D est stable par u. D est intersection de $n-1$ hyperplans de E, notons les $\mathrm{H}_1,\dots,\mathrm{H}_{n-1}$. On peut alors considérer les intersections de $n-r$ de ces hyperplans, par exemple $\mathrm{E}_1 = \mathrm{H}_1\cap\cdots\cap\mathrm{H}_{n-r}$, …, $\mathrm{E}_r = \mathrm{H}_r\cap\cdots\cap\mathrm{H}_{n-1}$, qui sont des espaces de dimension r. Donc chacun des E_i est laissé fixe par u, et il en est donc de même de leur intersection, qui n'est autre que D. u laisse donc chaque droite fixe : c'est une homothétie.

Exercice 6.

1. Une application classique de l'algorithme du pivot de Gauss montre [1] que si k est un corps, $\mathrm{E}_n(k) = \mathrm{SL}_n(k)$. Voir par exemple Lang, *Algebra*, XIII, §.9.
2. Si $\mathrm{A}\notin\mathrm{M}_2(k)$, on peut écrire $\mathrm{A} = \begin{pmatrix} a & b \\ c & d\end{pmatrix} = \begin{pmatrix} \mathrm{FD}(a)+a' & \mathrm{FD}(b)+b' \\ \mathrm{FD}(c)+c' & \mathrm{FD}(d)+d'\end{pmatrix}$, où a' est de degré strictement inférieur à $\mathrm{FD}(a)$ (et *idem* pour b, c et d) et où au moins l'un des coefficients de $\mathrm{FD}(\mathrm{A})$ n'est pas dans k.
   Comme l'inégalité $\deg\det\mathrm{A} = \deg(ad-bc) \leq \max(\deg ad, \deg bc)$ est stricte (ici, deg est le degré total), c'est que les termes dominants de ad et bc sont égaux. On a donc $\mathrm{FD}(ad) = \mathrm{FD}(bc)$ et $\det\mathrm{FD}(\mathrm{A}) = \mathrm{FD}(a)\mathrm{FD}(d) - \mathrm{FD}(b)\mathrm{FD}(c) = \mathrm{FD}(ad) - \mathrm{FD}(bc) = 0$.
3. Par définition, A s'écrit $\mathrm{A} = \mathrm{E}_1\cdots\mathrm{E}_m$, où chaque E_i est de la forme $\begin{pmatrix} 1 & f \\ 0 & 1\end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 \\ f & 1\end{pmatrix}$.
   On va démontrer le résultat par récurrence sur m. Le cas $m=1$ est évident : $\mathrm{A} = \mathrm{E}_1$ a un coefficient nul.
   Supposons donc le résultat démontré pour $m-1$ et posons

$$\mathrm{A}' = \begin{pmatrix} a & b \\ c & d\end{pmatrix} = \mathrm{E}_1\cdots\mathrm{E}_{m-1}\in\mathrm{E}_2(\mathrm{R}).$$

   D'après l'hypothèse de récurrence, trois choses peuvent arriver :

1. Notons que ce résultat est plus fort que celui donné en cours selon lequel *toutes* les transvections, et pas seulement les $1+xe_{ij}$, engendrent $\mathrm{SL}_n(k)$.

i. L'un des coefficients de A' est nul, disons $c = 0$ (les autres cas sont similaires). On a alors $\mathrm{A}' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et $\det \mathrm{A}' = 1$ implique $ad = 1$ et $a,\, d \in \mathrm{R}^* = \mathrm{A}^*$.

Si $\mathrm{E}_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, $\mathrm{A} = \mathrm{A}'\mathrm{E}_m$ garde un coefficient nul en bas à gauche. Il reste donc surtout à traiter le cas $\mathrm{E}_m = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$. Dans ce cas, $\mathrm{A} = \begin{pmatrix} a+bf & b \\ df & d \end{pmatrix}$.

Déjà, si $b = 0$ ou $f = 0$, la matrice A a un coefficient nul et le résultat est démontré. On peut donc supposer b et f non nuls. Si bf était un élement non nul de k, il en serait de même de b, de f et donc de df ; la matrice A serait donc à coefficients dans k, ce qui est exclu par hypothèse. On a donc $bf \notin k$, ce qui permet de déterminer la forme dominante de A : $\mathrm{FD}(\mathrm{A}) = \begin{pmatrix} \mathrm{FD}(b)\mathrm{FD}(f) & \mathrm{FD}(b) \\ d\mathrm{FD}(f) & d \end{pmatrix}$. La première ligne de cette matrice valant $\mathrm{FD}(b)/d$ fois la seconde, le résultat est démontré.

ii. $\mathrm{A}' \in \mathrm{M}_2(k)$ n'a aucun coefficient nul : $a,\, b,\, c,\, d \in k^*$.

Supposons en outre $\mathrm{E}_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$ (l'autre cas est similaire). On a alors $\mathrm{A} = \begin{pmatrix} a & af+c \\ c & cf+d \end{pmatrix}$. Comme A est supposée ne pas appartenir à $\mathrm{M}_2(k)$, on a $f \notin k$ et $\mathrm{FD}(\mathrm{A}) = \begin{pmatrix} a & af \\ c & cf \end{pmatrix}$. La première ligne de $\mathrm{FD}(\mathrm{A})$ est donc a/c fois la seconde et le résultat est démontré.

iii. L'une des lignes de $\mathrm{FD}(\mathrm{A}')$ est multiple de l'autre, disons

$$(\mathrm{FD}(a), \mathrm{FD}(b)) = h(\mathrm{FD}(c), \mathrm{FD}(d)) \text{ (l'autre cas est similaire).}$$

Supposons en outre $\mathrm{E}_m = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, donc $\mathrm{A} = \begin{pmatrix} a & af+b \\ c & cf+d \end{pmatrix}$. D'après la question précédente, $\det \mathrm{FD}(\mathrm{A}) = 0$. On a donc

$$\mathrm{FD}(c)\mathrm{FD}(af+b) = \mathrm{FD}(a)\mathrm{FD}(cf+d) = h\mathrm{FD}(c)\mathrm{FD}(cf+d),$$

ce qui implique $\mathrm{FD}(af+b) = h\mathrm{FD}(cf+b)$. On a alors la relation de proportionnalité voulue $(\mathrm{FD}(a), \mathrm{FD}(af+b)) = h(\mathrm{FD}(c), \mathrm{FD}(cf+d))$. Le cas $\mathrm{E}_m = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$ est similaire.

4. La matrice de Cohn a pour forme dominante $\mathrm{FD}(\mathrm{C}) = \begin{pmatrix} xy & x^2 \\ -y^2 & -xy \end{pmatrix}$. Aucun des deux vecteurs (xy, x^2) et $(-y^2, -xy)$ n'est multiple de l'autre. La question précédente implique $\mathrm{C} \notin \mathrm{E}_2(\mathrm{R})$, même si $\det \mathrm{C} = (1+xy)(1-xy) + x^2y^2 = 1$.

Exercice 7.

1. Le nombre de 7-sous-groupes de Sylow doit diviser $24 = 168/7$, et être congru à 1 modulo 7 (sans être 1, car G est simple) : c'est 8. L'action de G sur $\mathrm{Syl}_7(\mathrm{G})$ est transitive, donc l'équation aux classes donne le cardinal des stabilisateurs : $|\mathrm{N}| = |\mathrm{G}|/8 = 21$.
2. P agit par conjugaison sur $\mathrm{Syl}_7(\mathrm{G})$ en fixant P donc il agit sur $\mathrm{Syl}_7(\mathrm{G}) \setminus \{\mathrm{P}\}$. Les cardinaux des orbites pour cette action divisent $|\mathrm{P}| = 7$, ils sont donc égaux à 1 ou 7. Comme $|\mathrm{Syl}_7(\mathrm{G})| = 7$, s'il existait une orbite qui soit un singleton, ce serait également le cas de toutes les autres, et le noyau du morphisme $\mathrm{G} \longrightarrow \mathrm{Bij}(\mathrm{Syl}_7(\mathrm{G}))$ donné par

l'action de G par conjugaison contiendrait P. Comme G est simple, ce serait G tout entier. L'action serait alors triviale, ce qui est absurde car le théorème de Sylow garantit qu'elle est transitive. Il y a donc une seule orbite de cardinal 7, et le stabilisateur de chacun des points est de cardinal 1 : l'action est libre et transitive.

3. L'action de G sur les 7-sous-groupes de Sylow est fidèle car G est simple, donc il se plonge dans $\mathrm{Bij}(\mathrm{Syl}_7(\mathrm{G})) \simeq \mathfrak{S}_8$. Or, tout élément $\gamma \in \mathfrak{S}_8$ se décompose en produit de cycles de supports disjoints, son ordre étant alors le ppcm de la longueur de ces cycles. En utilisant que la somme des longueurs de cycles est plus petite que 8, nous obtenons le résultat, à savoir que l'ordre de tout élément est inférieur à 15. Si N était cyclique, on aurait dans G un élément d'ordre $21 > 15$, ce qui est exclu par la question précédente.
   A priori, N peut avoir un ou sept 3-sous-groupes de Sylow (qui sont des groupes C_3, cycliques d'ordre 3). S'il en a un seul, ce dernier est distingué dans N. Or, d'après le théorème de Sylow, le seul 7-sous-groupe de Sylow de N (isomorphe à C_7) est aussi distingué dans N. Si N n'avait qu'un seul 3-sous-groupe de Sylow, il serait alors isomorphe au produit direct $\mathrm{C}_3 \times \mathrm{C}_7 \simeq \mathrm{C}_{21}$, c'est-à-dire cyclique. Ce cas est donc exclu, ce qui entraîne $|\mathrm{Syl}_3(\mathrm{N})| = 7$.
4. Soit α, β, γ tels que $\mathrm{N} = \mathrm{P}\alpha \sqcup \mathrm{P}\beta \sqcup \mathrm{P}\gamma$. Pour $p \in \mathrm{P}$, $p\alpha$ normalise P' si et seulement si la conjugaison par p envoie $\alpha\mathrm{P}'\alpha^{-1}$ sur P'. D'après la deuxième question, cela arrive pour un unique p. Chacune des trois P-classes à droite de N rencontre donc N' en un seul élément, d'où $|\mathrm{M}| = |\mathrm{N} \cap \mathrm{N}'| = 3$.
5. $|\mathrm{Syl}_3(\mathrm{G})|$ est congru à 1 modulo 3 et divise $56 = 168/3$. Comme en outre G est simple, $|\mathrm{Syl}_3(\mathrm{G})|$ ne peut pas valoir 1. Donc $|\mathrm{Syl}_3(\mathrm{G})| \in \{4, 7, 28\}$. On a vu que N contenait déjà sept groupes d'ordre 3, donc $|\mathrm{Syl}_3(\mathrm{G})| \neq 4$. De même, si $|\mathrm{Syl}_3(\mathrm{G})| = 7$, tous les 3-sous-groupes de Sylow de G seraient contenus dans N. Par symétrie, ils seraient également contenus dans N', ce qui contredit $|\mathrm{N} \cap \mathrm{N}'| = 3$. On a donc bien $|\mathrm{Syl}_3(\mathrm{G})| = 28$.
6. Pour l'action de G par conjugaison sur ses 3-sous-groupes de Sylow, H est le stabilisateur de M, donc $|\mathrm{H}| = 168/28 = 6$.
   Les éléments d'ordre 3 ou 7 de G sont faciles à compter : comme $v_3(168) = 1$, les 3-sous-groupes de Sylow sont des groupes cycliques d'ordre 3, dont les intersections deux à deux sont triviales. les éléments d'ordre 3 sont exactement les éléments non triviaux de ces sous-groupes de Sylow. Comme $v_7(168) = 1$, on a un résultat analogue pour les 7-sous-groupes de Sylow.
   Il y a donc d'après les questions précédentes $8 \times (7-1) = 48$ éléments d'ordre 7 et $28 \times (3-1) = 56$ éléments d'ordre 3 dans G.
   Ensuite, remarquons que H est égal à son propre normalisateur dans G : si $g \in \mathrm{G}$ vérifie $g\mathrm{H}g^{-1} = \mathrm{H}$, $g\mathrm{M}g^{-1}$ est un sous-groupe de H de cardinal 3, donc $g\mathrm{M}g^{-1} = \mathrm{M}$ (un groupe d'ordre 6 ne contient qu'un seul sous-groupe d'indice 2) et $g \in \mathrm{H}$. Il y a donc $168/6 = 28$ conjugués de H dans G.
   Si H était cyclique, il contiendrait $\varphi(6) = 2$ éléments d'ordre 6. Avec ses conjugués, cela donnerait $28 \times 2 = 56$ éléments d'ordre 6 dans G (il n'y a pas de redondance possible : les éléments d'ordre 6 étant générateurs, ils ne peuvent appartenir qu'à un seul sous-groupe d'ordre 6). Comme $48 + 56 + 56 = 160$, il ne resterait que 8 éléments dont l'ordre soit susceptible de diviser 8. Il n'y aurait alors qu'un seul 2-sous-groupe de Sylow, ce qui n'est pas possible puisque G est simple. H ne peut donc pas être cyclique.
7. On a $\mu \in \mathrm{M} \subset \mathrm{N}_\mathrm{G}(\mathrm{P}) = \mathrm{N}$, et donc $\mu\pi\mu^{-1} \in \mathrm{P}$, d'où l'existence de n. Par récurrence, on a $\mu^k\pi\mu^{-k} = \pi^{n^k}$. Puisque M est d'ordre 3, $\mu^3 = 1$ donc $n^3 \equiv 1 \pmod 7$: n est une racine cubique de l'unité dans $\mathbf{F}_7$ soit, après vérification, 1, 2 ou 4.
   Les élements π (d'ordre 7) et μ (d'ordre 3) appartiennent à N (d'ordre 21) : ils engendrent donc N. Si n était égal à 1, μ et π commuteraient, ce qui entraînerait que N soit un

groupe abélien d'ordre 21. Mais un tel groupe est cyclique, ce qui est exclu par la question 2. On a donc $\mu\pi\mu^{-1} = \pi^2$ ou π^4.

Si d'aventure on avait $\mu\pi\mu^{-1} = \pi^4$, cela entraînerait $\mu^{-1}\pi^4\mu = \pi$. L'élément π étant d'ordre 7, cette relation entraîne $\mu^{-1}\pi\mu = \left(\mu^{-1}\pi^4\mu\right)^2 = \pi^2$. Quitte à remplacer μ par son inverse, on peut donc sypposer que $\mu\pi\mu^{-1} = \pi^2$. Puisque par ailleurs la conjugaison par π fixe évidemment P, cela entraîne que la conjugaison par π agit sur $\mathrm{Syl}_7(\mathrm{G}) = \mathbf{P}^1(\mathbf{F}^7)$ comme $x \mapsto 2x$.

8. τ appartient à $\mathrm{H} = \mathrm{N}_\mathrm{G}(\mathrm{M})$. La conjugaison par τ se restreint donc en un automorphisme de N. En particulier, $\tau\mu\tau^{-1}$ est un générateur de M, qui ne peut donc être que μ ou μ^{-1}. Mais, comme à la question précédente, le premier cas entraînerait que μ et τ commutent et donc que H soit cyclique, ce qui est exclu par la question 6. Donc $\tau\mu\tau^{-1} = \mu^{-1}$.

   Si l'action de τ sur $\mathrm{Syl}_7(\mathrm{G})$ avait un point fixe, τ normaliserait un 7-sous-groupe de Sylow. Il appartiendrait alors à son normalisateur. Mais τ est d'ordre 2 (Déjà, son ordre divise 6, mais ne peut pas être 6 car H n'est pas cyclique. Ensuite, $\mathrm{M} \lhd \mathrm{H}$ est l'unique 3-sous-groupe de Sylow, donc $\tau \in \mathrm{H} \setminus \mathrm{M}$ n'est pas d'ordre 3. On montrerait en fait assez vite que $(\mathrm{M}, \mathrm{H}) \simeq (\mathfrak{S}_3, \mathfrak{A}_3)$). Comme on a vu que les normalisateurs des 7-sous-groupes de Sylow sont d'ordre 21, τ ne pas pas appartenir à l'un d'eux. τ agit donc sans point fixe sur $\mathrm{P}^1(\mathbf{F}_7)$.

   Puisque μ agit comme $x \mapsto 2x$, on obtient les décompositions en cycles disjoints

$$\begin{aligned}
\widetilde{\mu} &= (0)(1\,2\,4)(3\,6\,5)(\infty) \\
\widetilde{\tau}\widetilde{\mu}\widetilde{\tau}^{-1} &= (\widetilde{\tau}(0))\,(\widetilde{\tau}(1)\,\widetilde{\tau}(2)\,\widetilde{\tau}(4))\,(\widetilde{\tau}(3)\,\widetilde{\tau}(6)\,\widetilde{\tau}(5))\,(\widetilde{\tau}(\infty)) \\
\widetilde{\mu}^{-1} &= (0)(1\,4\,2)(3\,5\,6)(\infty).
\end{aligned}$$

   (On remarquera que 1, 2 et 4 sont exactement les carrés non nuls modulo 7). Mais les deux dernières permutations sont égales ! Comme en outre $\widetilde{\tau}$ doit être une involution sans point fixe, il vient les valeurs suivantes (remarquons que $\widetilde{\tau}$ ne peut pas préserver globalement d'ensemble à 3 éléments, donc $\alpha = \widetilde{\tau}(1) \in \{3, 5, 6\}$, c'est-à-dire que α est un non-carré dans $\mathbf{F}_7$).

$x \in \mathbf{P}^1(\mathbf{F}_7)$	0	1	2	3	4	5	6	∞
$\widetilde{\tau}(x)$ si $\alpha = 3$	∞	3	5	1	6	2	4	0
$\widetilde{\tau}(x)$ si $\alpha = 5$	∞	5	6	4	3	1	2	0
$\widetilde{\tau}(x)$ si $\alpha = 6$	∞	6	3	2	5	4	1	0

   On vérifie alors facilement que dans ces trois cas, la permutation $\widetilde{\tau}$ est bien $x \mapsto \alpha/x$.

9. On a une action fidèle de $\mathrm{PGL}_2(\mathbf{F}_7)$ sur $\mathbf{P}^1(\mathbf{F}_7)$:

$$\begin{array}{ccc}
\mathrm{PGL}_2(\mathbf{F}_7) \times \mathbf{P}^1(\mathbf{F}_7) & \longrightarrow & \mathbf{P}^1(\mathbf{F}_7) \\
\left(\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right], x\right) & \mapsto & \begin{cases} \dfrac{ax+b}{cx+d} & \text{si } x \notin \{\infty, -d/c\} \\ \infty & \text{si } x = -d/c \\ a/c & \text{si } x = \infty \end{cases}
\end{array}$$

   Les diverses vérifications, faciles, ont été faites en partiel. On se permettra maintenant d'identifier $\mathrm{PGL}_2(\mathbf{F}_7)$ à l'image du morphisme associé $\mathrm{PGL}_2(\mathbf{F}_7) \to \mathrm{Bij}(\mathbf{P}^1(\mathbf{F}_7))$, dont les éléments sont appelés *homographies*.

   Commençons par montrer que la classe de $\mathrm{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{PGL}_2(\mathbf{F}_7)$ appartient à $\mathrm{PSL}_2(\mathbf{F}_7)$ si et seulement si $\det \mathrm{M}$ est un carré non nul de $\mathbf{F}_7$, autrement dit si $\det \mathrm{M} \in \{1, 2, 4\}$. En effet

$$[\mathrm{M}] \in \mathrm{PSL}_2(\mathbf{F}_7) \Leftrightarrow \exists \lambda \in \mathbf{F}_7^*, \mathrm{N} \in \mathrm{SL}_2(\mathbf{F}_7) : \mathrm{M} = \lambda \mathrm{N} \Leftrightarrow \exists \lambda \in \mathbf{F}_7^*, \det \mathrm{M} = \lambda^2.$$

Les trois permutations $\widetilde{\pi} : x \mapsto x+1$, $\widetilde{\mu} : x \mapsto 2x$ et $\widetilde{\tau} : x \mapsto \alpha/x$ pour un certain non-carré $\alpha \in \mathbf{F}_7$ sont des homographies. On les obtient comme les éléments de $\mathrm{PGL}_2(\mathbf{F}_7)$ correspondant aux matrices $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\begin{pmatrix}2&0\\0&1\end{pmatrix}$ et $\begin{pmatrix}0&\alpha\\1&0\end{pmatrix}$, respectivement. Ces trois matrices sont de déterminant carré (1, 2 et $-\alpha$, respectivement). L'action de G sur $\mathrm{Syl}_7(\mathrm{G})$ fournit donc en fait un morphisme (injectif car G est simple)

$$\Phi : \mathrm{G} \longrightarrow \mathrm{Bij}(\mathbf{P}^1(\mathbf{F}_7))$$

envoyant $\langle \pi, \mu, \tau \rangle$ dans $\mathrm{PSL}_2(\mathbf{F}_7)$.

On va montrer que $\widetilde{\pi}$, $\widetilde{\mu}$ et $\widetilde{\tau}$ engendrent $\mathrm{PSL}_2(\mathbf{F}_7)$. Il s'ensuivra alors que Φ réalise un isomorphisme entre $\langle \pi, \mu, \tau \rangle$ et $\mathrm{PSL}_2(\mathbf{F}_7)$. Comme $\langle \pi, \mu, \tau \rangle \subseteq \mathrm{G}$ et que G est d'ordre $168 = |\mathrm{PSL}_2(\mathbf{F}_7)|$, on aura bien $\mathrm{G} = \langle \pi, \mu, \tau \rangle \simeq \mathrm{PSL}_2(\mathbf{F}_7)$.

Le sous-groupe $\langle \widetilde{\pi}, \widetilde{\mu}, \widetilde{\tau} \rangle$ contient déjà les homographies $\mathrm{T}_k : x \mapsto x+k$ pour $k \in \mathbf{F}_7$, $\mathrm{D}_\gamma : x \mapsto \gamma x$ pour γ carré dans $\mathbf{F}_7^*$ et $\mathrm{I}_\beta : x \mapsto \beta/x$ pour α non carré dans $\mathbf{F}_7^*$. Soit maintenant $z \mapsto \dfrac{az+b}{cz+d}$, $ad-bc=1$ une homographie dans $\mathrm{PSL}_2(\mathbf{F}_7)$.

- Si $c = 0$, l'homographie s'écrit $z \mapsto \dfrac{a}{d}z + \dfrac{b}{d} = a^2 z + \dfrac{b}{d}$ (car $ad = 1$ et on peut bien l'écrire sous la forme $\mathrm{T}_{b/d} \circ \mathrm{D}_{a^2}$.
- Sinon, elle s'écrit $z \mapsto \dfrac{-1/c^2}{z + d/c} + \dfrac{a}{c}$, c'est-à-dire sous la forme $\mathrm{T}_{a/c} \circ \mathrm{I}_{-1/c^2} \circ \mathrm{T}_{d/c}$, ce qui est légitime car $-1/c^2$ n'est pas un carré dans $\mathbf{F}_7$.

10. $\mathrm{GL}_3(\mathbf{F}_2) = \mathrm{PSL}_3(\mathbf{F}_2)$ est simple et d'ordre $(2^3-1)(2^3-2)(2^3-2^2) = 168$.

Exercice 8.

1. Commençons par remarquer que pour tout $i \in [\![1, n]\!]$, $\mathrm{W}_i \not\subset \mathrm{W}_{i-1} + \mathrm{V}_{s(i)-1}$. C'est la définition de $s(i)$ comme minimum si $s(i) \neq 1$ et une tautologie si $s(i) = 1$: W_i ne peut pas être inclus dans $\mathrm{W}_{i-1} + \mathrm{V}_0 = \mathrm{W}_{i-1}$.

   On peut donc trouver un élément $x_i \in \mathrm{W}_i \setminus (\mathrm{W}_{i-1} + \mathrm{V}_{s(i)-1})$. Puisque $\mathrm{W}_i \subset \mathrm{W}_{i-1} + \mathrm{V}_{s(i)}$, on peut décomposer cet élément en $x_i = w_i + v_i$ avec $w_i \in \mathrm{W}_{i-1}$ et $v_i \in \mathrm{V}_{s(i)}$. Montrons que v_i vérifie les conditions demandées.

   Déjà, $v_i = x_i - w_i$ appartient à W_i. En outre, s'il était dans W_{i-1}, on aurait $x_i \in \mathrm{W}_{i-1}$ ce qui est exclu. On a donc $v_i \in \mathrm{W}_i \setminus \mathrm{W}_{i-1}$ et un argument de dimension montre que $\mathrm{W}_i = \mathrm{W}_{i-1} \oplus \mathrm{K}v_i$.

   Ensuite, par construction $v_i \in \mathrm{V}_{s(i)}$. S'il était dans $\mathrm{V}_{s(i)-1}$, on aurait $x_i \in \mathrm{W}_{i-1} + \mathrm{V}_{s(i)-1}$, ce qui est exclu. On a donc $v_i \in \mathrm{V}_{s(i)} \setminus \mathrm{V}_{s(i)-1}$ et un argument de dimension montre que $\mathrm{V}_{s(i)} = \mathrm{W}_{s(i)-1} \oplus \mathrm{K}v_i$.

   Enfin, si v_i appartenait à $\mathrm{W}_{i-1} + \mathrm{V}_{s(i)-1}$, x_i appartiendrait également à cet espace, ce qui est exclu. On a donc vérifié les trois propriétés.

2. On va démontrer que l'application $t = s_{\mathbf{W},\mathbf{V}}$ est un inverse de s. D'après les propriétés des applications d'un ensemble fini dans lui-même, il suffit de démontrer que c'en est un inverse à gauche, c'est-à-dire que $t \circ s = \mathrm{id}_{[\![1,n]\!]}$.

   Soit donc $i \in [\![1, n]\!]$ et $j = s(i)$.

   On a à la fois $\mathrm{W}_i = \mathrm{W}_{i-1} \oplus \mathrm{K}v_i$ et $\mathrm{V}_j = \mathrm{V}_{j-1} \oplus \mathrm{K}v_i$. On a donc bien $\mathrm{V}_j \subset \mathrm{V}_{j-1} + \mathrm{W}_i$ et $\mathrm{V}_j \not\subset \mathrm{V}_{j-1} + \mathrm{W}_{i-1}$. Cela démontre bien que $i = t(j)$.

   Il reste à démontrer que toute permutation est de cette forme. Soit $\mathbf{V} = \mathbf{F}_{\mathrm{can}}$ le drapeau canonique, c'est-à-dire le drapeau dont le i-ème espace est $\mathrm{Vect}(e_1, \ldots, e_i)$, où (e_i) est

la base canonique de K^n et, pour $\sigma \in \mathfrak{S}_n$, $\mathbf{W} = \mathbf{F}_\sigma$ le drapeau dont le i-ème espace est $\mathrm{Vect}(e_{\sigma(1)}, \dots, e_{\sigma(n)})$. On a

$$\begin{aligned} \mathrm{W}_i \subset \mathrm{W}_{i-1} + \mathrm{V}_j &\Leftrightarrow \{\sigma(1), \dots, \sigma(i)\} \subset \{\sigma(1), \dots, \sigma(i-1)\} \cup [\![1, j]\!] \\ &\Leftrightarrow \sigma(i) \in [\![1, j]\!] \end{aligned}$$

donc $s_{\mathbf{V},\mathbf{W}}(i) = \min \left\{ j \in [\![1,n]\!] \,\middle|\, \sigma(i) \in [\![1,j]\!] \right\} = \sigma(i)$ et $s_{\mathbf{V},\mathbf{W}} = \sigma$.

3. Par construction, la famille (v_i) est telle que $\mathrm{W}_i = \mathrm{Vect}(e_1, \dots, e_i)$ et, puisque $\mathrm{V}_j = \mathrm{V}_{j-1} \oplus \mathrm{K}e_{t(j)}$, $\mathrm{V}_j = \mathrm{Vect}(e_{t(1)}, \dots, e_{t(j)})$. Cela démontre à la fois que la famille (v_i) est une base et qu'elle est adaptée aux deux drapeaux complets.

4. L'image d'un drapeau $\mathbf{V} = (\mathrm{V}_i)_{i=0}^n$ est simplement le drapeau $(g(\mathrm{V}_i))_{i=0}^n$. $\mathrm{GL}_n(\mathrm{K})$ agit sur l'ensemble Δ des couples de drapeaux par l'action diagonale :

$$g(\mathbf{V}, \mathbf{W}) = (g(\mathbf{V}), g(\mathbf{W})).$$

Déjà, la définition de la permutation $s_{\mathbf{V},\mathbf{W}}$ rend manifeste que c'est un *invariant* de l'action : pour $g \in \mathrm{GL}_n(\mathrm{K})$, on a $s_{g(\mathbf{V},\mathbf{W}} = s_{\mathbf{V},\mathbf{W}}$. On a donc une application

$$\Phi : \begin{array}{ccc} \Delta/\mathrm{GL}_n(\mathrm{K}) & \to & \mathfrak{S}_n \\ [(\mathbf{V}, \mathbf{W})] & \mapsto & s_{(\mathbf{V},\mathbf{W})} \end{array}$$

bien définie. Elle est surjective d'après la question précédente : $\Phi([(\mathbf{F}_{\mathrm{can}}, \mathbf{F}_\sigma)]) = \sigma$.
Il reste à voir que cette application est injective. Pour cela, il suffit de montrer que deux couples de drapeaux définissant la même permutation sont dans la même orbite sous $\mathrm{GL}_n(\mathrm{K})$. Il suffit donc même de démontrer que tout couple de drapeaux est dans l'orbite de $(\mathbf{F}_{\mathrm{can}}, \mathbf{F}_\sigma)$ pour un certain σ (qui ne pourra alors qu'être la permutation s que ce couple définit). Soit donc $(\mathbf{V}, \mathbf{W})$ un couple de drapeaux et (v_i) la famille définie à la question 1. Il existe alors un (unique) élément $g \in \mathrm{GL}_n(\mathrm{K})$ tel que $g(v_{s^{-1}(i)}) = e_i$, le i-ème vecteur de la base canonique. Comme $\mathrm{V}_i = \mathrm{Vect}(v_{s^{-1}(1)}, \dots, v_{s^{-1}(n)})$ et $\mathrm{W}_i = \mathrm{Vect}(v_1, \dots, v_n)$ on a $g(\mathrm{V}_i) = \mathrm{Vect}(e_1, \dots, e_n)$ et $g(\mathrm{W}_i) = \mathrm{Vect}(e_{s(1)}, \dots, e_{s(n)})$, c'est-à-dire $g(\mathbf{V}, \mathbf{W}) = (\mathbf{F}_{\mathrm{can}}, \mathbf{F}_\sigma)$. L'application Φ est donc une bijection et l'action de $\mathrm{GL}_n(\mathrm{K})$ a $|\mathfrak{S}_n| = n!$ orbites.

5. Soit $g \in \mathrm{GL}_n\mathrm{K}$ et $\mathbf{G} = g(\mathbf{F}_{\mathrm{can}})$. D'après la question précédente, il existe une unique permutation $\sigma \in \mathfrak{S}_n$ telle que $(\mathbf{F}_{\mathrm{can}}, \mathbf{G})$ et $(\mathbf{F}_{\mathrm{can}}, \mathbf{F}_\sigma)$ soient dans la même orbite.

6. Soit $g \in \mathrm{GL}_n(\mathrm{K})$. Soit $\mathbf{G} = g(\mathbf{F}_{\mathrm{can}})$. D'après la question précédente, il existe $\sigma \in \mathfrak{S}_n$ et $h \in \mathrm{GL}_n(\mathrm{K})$ tels que $h(\mathbf{F}_{\mathrm{can}}, \mathbf{G}) = (\mathbf{F}_{\mathrm{can}}, \mathbf{F}_\sigma)$. Si on note P_σ la matrice de permutation telle que $\mathrm{P}_\sigma(\mathbf{F}_{\mathrm{can}}) = \mathbf{F}_\sigma$, on a donc $h(\mathbf{F}_{\mathrm{can}}) = \mathbf{F}_{\mathrm{can}}$ et $hg(\mathbf{F}_{\mathrm{can}}) = \mathrm{P}_\sigma(\mathbf{F}_{\mathrm{can}})$, soit $(\mathrm{P}_\sigma^{-1} hg)(\mathbf{F}_{\mathrm{can}}) = \mathbf{F}_{\mathrm{can}}$. Puisque le sous-groupe B est précisément formé des éléments fixant le drapeau $\mathbf{F}_{\mathrm{can}}$, on a bien une décomposition de g de la forme voulue :

$$g = h^{-1}hg = \underbrace{h^{-1}}_{\in \mathrm{B}} \mathrm{P}_\sigma \underbrace{\mathrm{P}_\sigma^{-1} hg}_{\in \mathrm{B}}.$$

On a donc la décomposition $\mathrm{GL}_n(\mathrm{K}) = \bigcup_{w \in \mathrm{W}} \mathrm{B}w\mathrm{B}$. Pour démontrer l'unicité, remarquons que si $g = bwb'$, avec $w = \mathrm{P}_\sigma$, alors $b^{-1}g = wb'$ et $b^{-1}(g(\mathbf{F}_{\mathrm{can}})) = wb(\mathbf{F}_{\mathrm{can}}) = \mathbf{F}_\sigma$. On a donc à la fois $b(\mathbf{F}_{\mathrm{can}}) = \mathbf{F}_{\mathrm{can}}$ (car $b \in \mathrm{B}$) et $b(\mathbf{F}_\sigma) = g(\mathbf{F}_{\mathrm{can}})$. On a donc $b(\mathbf{F}_{\mathrm{can}}, \mathrm{F}_\sigma) = (\mathbf{F}_{\mathrm{can}}, g(\mathbf{F}_{\mathrm{can}}))$ ce qui entraîne $\sigma = s_{\mathbf{F}_{\mathrm{can}}, g(\mathbf{F}_{\mathrm{can}})}$: la permutation $\sigma \in \mathfrak{S}_n$ (et donc l'élément $w \in \mathrm{W}$) sont donc parfaitement déterminées par g. On a bien démontré la *décomposition de Bruhat* :

$$\mathrm{GL}_n(\mathrm{K}) = \bigsqcup_{w \in \mathrm{W}} \mathrm{B}w\mathrm{B}.$$