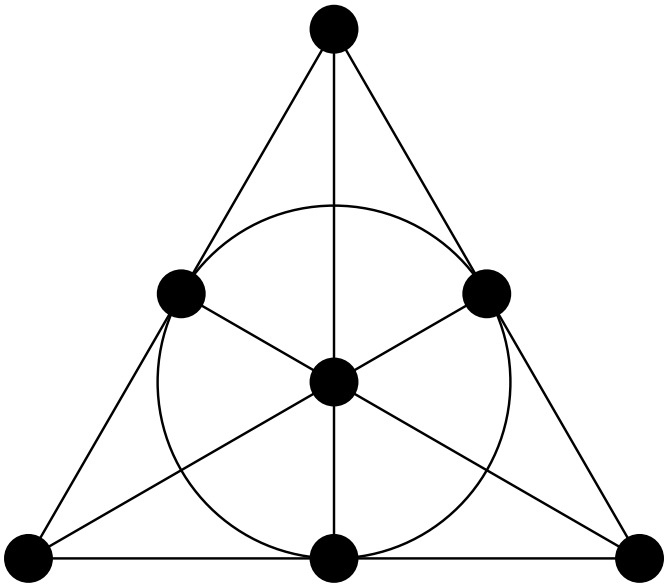
Le groupe simple d'ordre 168

Blaise Boissonneau

Avril 2017



Sommaire

Introduction

La classification des groupes simples d'ordre fini est un théorème affirmant que les groupes simples d'ordre fini sont soit cycliques d'ordre p premier, soit alternés de degré $n \geqslant 5$, soit membre d'une des 16 familles de groupes de type Lie, soit l'un des 27 groupes sporadiques. Ce théorème est souvent appelé le théroème énorme, en raison de la difficulté et de la longueur de sa démonstration ; à l'heure actuelle, la preuve la plus aboutie est en cours de rédaction, et pourrait tenir sur 5000 pages une fois terminée[1]. Le sujet de notre travail sera de démontrer la simplicité d'une famille particulière de groupes, les groupes projectifs spéciaux linéaires, aussi appelés les groupes de Chevalley linéaires, et d'étudier en détail deux d'entre eux, qui sont d'ordre 168, et dont on verra qu'ils sont isomorphes entre eux.

1 Étude du groupe général linéaire

1.1 Définitions et notations

Soit A un anneau commutatif non-nul. On notera $\mathfrak{M}_n(A)$ la A-algèbre des matrices carrées de taille $n \in \mathbb{N}^*$ à coefficients dans A, et $\mathfrak{M}_{n,p}(A)$ le A-module des matrices de dimension (n,p) à coefficients dans A. Pour toute matrice $M \in \mathfrak{M}_{n,p}$, on notera $\mathcal{L}_i(M)$ la i$^{\text{ème}}$ ligne et $\mathcal{C}_j(M)$ la j$^{\text{ème}}$ colonne de M ; et $C_{i,j}(M)$ le coefficient (i,j) de M.
On s'intéressera aux sous-ensembles suivants :

$\mathrm{GL}(n,A)$ **:** groupe multiplicatif des inversibles de la A-algèbre $\mathfrak{M}_n(A)$;

$\mathrm{SL}(n,A)$ **:** sous-groupe de $\mathrm{GL}(n,A)$ formé des matrices de déterminant 1_A ;

$\mathcal{H}(n,A)$ **:** A-algèbre formée des matrices λI_n avec $\lambda \in A$;

$\mathcal{H}^*(n,A)$ **:** groupe des éléments inversibles de $\mathcal{H}(n,A)$, c'est à dire les matrices λI_n avec λ inversible dans A ;

$\mathbf{S}\mathcal{H}^*(n,A)$ **:** $\mathrm{SL}(n,A) \cap \mathcal{H}^*(n,A)$.

Comme A est commutatif, $\mathcal{H}^*(n,A)$ est contenu dans le centre de $\mathrm{GL}(n,A)$, et $\mathrm{S}\mathcal{H}^*(n,A)$ dans le centre de $\mathrm{SL}(n,A)$; ce sont donc des sous-groupes distingués. On définira alors les groupes projectifs linéaires suivants :

$$\mathrm{PGL}(n,A) = \mathrm{GL}(n,A)/\mathcal{H}^*(n,A)\,;\ \mathrm{PSL}(n,A) = \mathrm{SL}(n,A)/\mathrm{S}\mathcal{H}^*(n,A)$$

Ils feront l'objet d'une étude précise dans la suite. Pour l'instant, nous allons définir différents types de matrices, et déterminer comment elles agissent par multiplication.

Base, transvections & dilatations Soit $(E_{i,j})_{1\leqslant i,j\leqslant n}$ la base canonique de $\mathfrak{M}_n(A)$ comme A-module : $C_{k,l}(E_{i,j}) = \delta_{k,i}\cdot\delta_{l,j}$, où δ est le symbole de Kronecker. On a alors :

$$E_{i,j} \times E_{k,l} = \delta_{j,k} E_{i,l}$$

Pour $\lambda \in A$, on définit la matrice dite *de dilatation* $D(\lambda) = \mathrm{Diag}(1, \dots, 1, \lambda)$, et on a $\det(D(\lambda)) = \lambda$.

Pour $\lambda \in A$ non nul et $i \neq j$, on définit la matrice dite *de transvection* $T_{i,j} = I_n + \lambda E_{i,j}$. Cette définition n'est valable que si $n \geqslant 2$. Alors :

- $T_{i,j}(\lambda)$ agit sur $M \in \mathfrak{M}_{n,p}(A)$ par multiplication à gauche en remplaçant $\mathcal{L}_i(M)$ par $\mathcal{L}_i(M) + \lambda \mathcal{L}_j(M)$;
- $T_{i,j}(\lambda)$ agit sur $M \in \mathfrak{M}_{p,n}(A)$ par multiplication à droite en remplaçant $\mathcal{C}_j(M)$ par $\mathcal{C}_j(M) + \lambda \mathcal{C}_i(M)$.

Enfin, $T_{i,j}(\lambda)$ est inversible d'inverse $T_{i,j}(-\lambda)$.

Ainsi, une suite de multiplications par des matrices de transvection revient à une suite d'opérations sur les lignes et les colonnes. Notamment, comme $\det(T_{i,j}(\lambda)) = 1$, ces opérations ne modifient pas le déterminant.

1.2 Générateurs

On se place dorénavant dans le cas où A est un corps commutatif, noté K, et où n est fixé.

Théorème 1.1. *Soit $M \in \mathrm{GL}(n, K)$. Posons $\lambda = \det(M)$, alors :*

(a) $\exists r \in \mathbb{N}^*$, $\exists A_1, \dots, A_r$ des matrices de transvections telles que :

$$M = D(\lambda) \times A_1 \times \cdots \times A_r$$

(b) $\exists s \in \mathbb{N}^*$, $\exists B_1, \dots, B_s$ des matrices de transvections telles que :

$$M = B_1 \times \cdots \times B_s \times D(\lambda)$$

Démonstration. On prouvera (a), la démonstration de (b) étant similaire. On procédera par récurrence : pour $n = 1$, $M = D(\lambda)$, et le résultat est prouvé. Pour $n > 1$, supposons le résultat vrai à l'ordre $n - 1$.

Soit $\mathcal{E} = \{M \times Q_1 \times \cdots \times Q_m \mid m \in \mathbb{N}^*, Q_k \text{ de transvection}\}$. Il est clair que $M \in \mathcal{E}$.

On sait que $\mathcal{L}_1(M) \neq 0$, car $\det(M) \neq 0$. Si $C_{1,2}(M) = 0$, alors $\exists j \in \{1 \dots n\}$, $j \neq i$ tel que $C_{1,j}(M) \neq 0$. Alors, $M_0 = M \times T_{j,2}(1)$ est telle que $C_{1,2}(M_0) \neq 0$, et $M_0 \in \mathcal{E}$.

Il y a donc dans $\mathcal{E}$ une matrice M_1 telle que $C_{1,2}(M_1) \neq 0$. Soit $\mu = \frac{1 - C_{1,1}(M_1)}{C_{1,2}(M_1)}$, alors $M_2 = M_1 \times T_{2,1}(\mu)$ est telle que $C_{1,1}(M_2) = 1$, et appartient à $\mathcal{E}$.

Soit désormais $M_3 = M_2 \times T_{1,2}(-C_{1,2}(M_2)) \times \cdots \times T_{1,n}(-C_{1,n}(M_2))$. $M_3 \in \mathcal{E}$ est telle que $C_{1,1}(M_3) = 1$ et $\forall j \in 2 \dots n$, $C_{1,j}(M_3) = 0$. Il y a donc dans $\mathcal{E}$ une

matrice M' de la forme :

$$M' = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline X & & N & \end{array}\right)$$

Avec $N \in \mathfrak{M}_{n-1}(K)$ et $X \in \mathfrak{M}_{n-1,1}(K)$.

Puisque la multiplication par une matrice de transvection ne modifie par le déterminant, $\det(M') = \det(N) = \lambda \neq 0$.

Ainsi, $X = N \times N^{-1} \times X = N \times \xi$, avec $\xi = N^{-1} \times X \in \mathfrak{M}_{n-1,1}$, que l'on peut réécrire $\mathcal{C}_1(M') - \mathcal{C}_1(I_n) = \sum_{i=1}^{n-1} \xi_i \mathcal{C}_{i+1}(M')$. Alors, $M'' = M' \times T_{2,1}(-\xi_1) \times T_{3,1}(-\xi_2) \times \cdots \times T_{n,1}(-\xi_{n-1}) \in \mathcal{E}$ est de la forme :

$$M'' = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & N & \\ 0 & & & \end{array}\right)$$

Pour $n = 2$, on s'arrête ici, car on a prouvé le résultat. Pour $n > 2$, on obtient par récurrence l'existence de $k \in \mathbb{N}^*$ et $W_1, \ldots, W_k \in \mathrm{GL}(n-1, K)$ de transvection tels que $N = \Delta \times W_1 \times \cdots \times W_k$, avec $\Delta = D(\lambda) \in \mathrm{GL}(n-1, K)$. On définit enfin pour $i \in \{1 \ldots k\}$:

$$U_i = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & W_i & \\ 0 & & & \end{array}\right)$$

U_i est de transvection, et on a $M'' = D(\lambda) \times U_1 \times \cdots \times U_k$, ce qui donne $D(\lambda) = M'' \times U_k^{-1} \times \cdots \times U_1^{-1} \in \mathcal{E}$, car l'inverse d'une matrice de transvection est de transvection. Pour cette même raison, $D(\lambda) \in \mathcal{E} \Leftrightarrow (a)$. □

Exemple On illustrera la méthode de construction à l'aide d'une matrice $M \in \mathrm{GL}(n, \mathbb{Q})$:

$$M = \begin{pmatrix} 2 & 0 & -2 \\ 0 & -4 & 9 \\ 6 & 2 & 0 \end{pmatrix}$$

Et l'on suivra son évolution à chaque multiplication par une matrice de transvection :

$$\left(\begin{array}{c|c|c} 2 & 0 & -2 \\ 0 & -4 & 9 \\ 6 & 2 & 0 \end{array}\right) \xrightarrow{\times T_{1,2}(1)} \left(\begin{array}{c|c|c} 2 & 2 & -2 \\ 0 & -4 & 9 \\ 6 & 8 & 0 \end{array}\right) \xrightarrow{\times T_{2,1}(-\frac{1}{2})} \left(\begin{array}{c|c|c} 1 & 2 & -2 \\ 2 & -4 & 9 \\ 2 & 8 & 0 \end{array}\right)$$

$$\xrightarrow{\times T_{1,2}(-2)} \left(\begin{array}{c|c|c} 1 & 0 & -2 \\ \hline 2 & -8 & 9 \\ \hline 2 & 4 & 0 \end{array}\right) \xrightarrow{\times T_{1,3}(2)} \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 2 & -8 & 13 \\ \hline 2 & 4 & 4 \end{array}\right)$$

Il nous faut désormais déterminer le vecteur $\xi \in \mathfrak{M}_{2,1}$:

$$\xi = \begin{pmatrix} -8 & 13 \\ 4 & 4 \end{pmatrix}^{-1} \times \begin{pmatrix} 2 \\ 2 \end{pmatrix} = -\frac{1}{84} \begin{pmatrix} 4 & -13 \\ -4 & -8 \end{pmatrix} \times \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} \frac{3}{14} \\ \frac{2}{7} \end{pmatrix}$$

Ainsi

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 2 & -8 & 13 \\ \hline 2 & 4 & 4 \end{array}\right) \xrightarrow{\times T_{2,1}(-\frac{3}{14}) \times T_{3,1}(-\frac{2}{7})} \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -8 & 13 \\ \hline 0 & 4 & 4 \end{array}\right)$$

On répète maintenant le procédé avec la sous-matrice d'ordre 2 obtenue :

$$\left(\begin{array}{c|c} -8 & 13 \\ \hline 4 & 4 \end{array}\right) \xrightarrow{\times T_{2,1}(\frac{9}{13})} \left(\begin{array}{c|c} 1 & 13 \\ \hline \frac{88}{13} & 4 \end{array}\right) \xrightarrow{\times T_{1,2}(-13)} \left(\begin{array}{c|c} 1 & 0 \\ \hline \frac{88}{13} & -84 \end{array}\right)$$

$$\xrightarrow{\times T_{2,1}(273)} \begin{pmatrix} 1 & 0 \\ 0 & -84 \end{pmatrix}$$

On obtient alors, en prenant soin de rajouter 1 aux indices des transvections effectuées pour la sous-matrice d'ordre 2, la formule suivante :

$$M \times T_{1,2}(1) \times T_{2,1}(-\tfrac{1}{2}) \times T_{1,2}(-2) \times T_{1,3}(2) \times T_{2,1}(-\tfrac{3}{14}) \times T_{3,1}(-\tfrac{2}{7})$$
$$\times T_{3,2}(\tfrac{9}{13}) \times T_{2,3}(-13) \times T_{3,2}(273) = D(-84)$$

Ou encore

$$M = D(-84) \times T_{3,2}(-273) \times T_{2,3}(13) \times T_{3,1}(-\tfrac{9}{13})$$
$$\times T_{3,1}(\tfrac{2}{7}) \times T_{2,1}(\tfrac{3}{14}) \times T_{1,3}(-2) \times T_{1,2}(2) \times T_{2,1}(\tfrac{1}{2}) \times T_{1,2}(-1)$$

Puisque $\mathrm{SL}(n, K)$ est le sous-groupe des matrices de déterminant 1, on obtient en applicant le théorème précédent :

Corollaire 1.1. $\mathrm{SL}(n, K)$ *est engendré par les matrices de transvections.*

1.3 Centralisateurs et commutants

Soit G un groupe et $E \subset G$. On définit $\mathcal{Z}_G(E)$ le centralisateur de E dans G par $\mathcal{Z}_G(E) = \{g \in G \mid \forall x \in E,\ gx = xg\}$. C'est un sous-groupe de G.

Soit A un anneau commutatif et $\mathcal{A}$ une A-algèbre associative et unifère, pour une partie E de $\mathcal{A}$, on définit $C_{\mathcal{A}}(E)$ le commutant de E dans $\mathcal{A}$ par $C_{\mathcal{A}}(E) = \{a \in \mathcal{A} \mid \forall x \in E,\ ax = xa\}$. C'est une sous-algèbre de $\mathcal{A}$, qui contient les homothéties de $\mathcal{A}$ [1] car A est commutatif.
Si E est inclus dans $\mathcal{U}(\mathcal{A})$, alors $C_{\mathcal{A}}(E) \cap \mathcal{U}(A) = \mathcal{Z}_{\mathcal{U}(A)}(E)$.

$C_{\mathcal{A}}(\mathcal{A})$ se note simplement $C(\mathcal{A})$ et s'appelle le centre de $\mathcal{A}$.

1. On rappelle que les homothéties de $\mathcal{A}$ sont les éléments de la forme $\lambda 1_{\mathcal{A}}$.

Théorème 1.2.

$$\mathcal{Z}_{\mathrm{GL}(n,K)}(\mathrm{SL}(n,K)) = \mathcal{H}^*(n,K),\ \textit{et}\ C_{\mathfrak{M}_n(K)}(SL(n,K)) = \mathcal{H}(n,K).$$

Démonstration. La première égalité découle de la deuxième ; en effet, on a $\mathcal{Z}_{\mathrm{GL}(n,K)}(\mathrm{SL}(n,K)) = C_{\mathfrak{M}_n(K)}(SL(n,K)) \cap \mathrm{GL}(n,K)$, par inclusion de $\mathrm{SL}(n,K)$ dans $\mathrm{GL}(n,K) = \mathcal{U}(\mathfrak{M}_n(K))$.

Soit $M \in C_{\mathfrak{M}_n(K)}(SL(n,K))$. Puisque $\mathrm{SL}(n,K)$ est engendré par les matrices de transvection, M commute avec chaque matrice de transvection. Ainsi pour j fixé, $M \times T_{1,j}(1_K) = T_{1,j}(1_K) \times M$, ou encore $C_{1,1}(M) = C_{j,j}(M)$ et $C_{j,k}(M) = 0$ pour $k \neq j$. En faisant varier j, on obtient $M = C_{1,1}(M)I_n \in \mathcal{H}(n,K)$. □

On sait que $\mathcal{H}^*(n,K) \subset \mathcal{Z}(\mathrm{GL}(n,K))$, on a désormais $\mathcal{Z}(\mathrm{GL}(n,K)) \subset \mathcal{Z}_{\mathrm{GL}(n,k)}(\mathrm{SL}(n,K)) = \mathcal{H}^*(n,K)$, donc :

Corollaire 1.2.

$$\mathcal{Z}(\mathrm{GL}(n,K)) = \mathcal{H}^*(n,K),\ \textit{et}\ \mathcal{Z}(\mathrm{SL}(n,K)) = \mathcal{H}^*(n,K) \cap \mathrm{SL}(n,K).$$

On notera que $\mathcal{H}^*(n,K) \cap \mathrm{SL}(n,K) = \mathrm{S}\mathcal{H}^*(n,K) = \{\lambda I_n \mid \lambda \in K,\ \lambda^n = 1_K\}$. Le corollaire suivant est moins trivial, et nous intéresse beaucoup plus :

Corollaire 1.3.

$$\mathcal{Z}(\mathrm{PGL}(n,K))\ \textit{et}\ \mathcal{Z}(\mathrm{PSL}(n,K))\ \textit{sont réduits à l'élément neutre.}$$

Démonstration. On notera $M \to \overline{M}$ la surjection canonique de $\mathrm{GL}(n,K)$ dans $\mathrm{PGL}(n,K) = \mathrm{GL}(n,K)/\mathcal{H}^*(n,K)$. Soit $\overline{M} \in \mathcal{Z}(\mathrm{PGL}(n,K))$. Alors, pour $N \in \mathrm{GL}(n,K)$ quelconque, $\overline{M} \times \overline{N} \times \overline{M}^{-1} \times \overline{N}^{-1} = \overline{N} \times \overline{M} \times \overline{M}^{-1} \times \overline{N}^{-1} = \overline{I_n}$, c'est-à-dire $M \times N \times M^{-1} \times N^{-1} \in \mathcal{H}^*(n,K)$. On définit alors $f : \mathrm{GL}(n,K) \to K^*$ par $f(N) = C_{1,1}(M \times N \times M^{-1} \times N^{-1})$.

Nous allons montrer que M est une matrice diagonale. Pour ce faire, fixons i et $j \in \{1,\ldots,n\}$ distincts. On note pour $\rho \in K^*$ quelconque, $\lambda(\rho) = f(T_{i,j(\rho)})$, alors $M \times T_{i,j}(\rho) = \lambda(\rho)T_{i,j}(\rho) \times M$, ce qui donne pour $k \neq j : C_{i,k}(M \times T_{i,j}(\rho)) = C_{i,k}(\lambda(\rho)T_{i,j}(\rho) \times M)$, ou encore $C_{i,k}(M) = \lambda(\rho)(C_{i,k}(M) + \rho C_{j,k}(M))$.
Si $C_{j,k}(M) \neq 0$, alors pour $\rho = \rho_k = -\frac{C_{i,k}(M)}{C_{j,k}(M)}$, on a $C_{i,k}(M) = 0$, ce qui donne $\lambda(\rho) = 0$ pour $\rho \neq \rho_k$. Mais $\lambda(\rho) \in K^*$ et $|K| \geqslant 2$, ce qui donne une contradiction. Alors $C_{j,k}(M) = 0$ pour $k \neq j$, $\forall j \in \{1,\ldots,n\} : M$ est diagonale.
Posons désormais $N_1 = \left(\begin{array}{c|c} 1 \quad \ldots \quad 1 & \\ \hline 0 & \\ \vdots & I_{n-1} \\ 0 & \end{array}\right) \in \mathrm{SL}(n,K)$, et $\lambda_1 = f(N_1)$.
On a $M \times N_1 = \lambda_1 N_1 \times M$, donc pour i fixé, $C_{1,i}(M \times N_1) = \lambda_1 C_{1,i}(N_1 \times M)$, ou encore $C_{1,1}(M) = \lambda_1 C_{i,i}(M)$. On obtient $\lambda_1 = 1$ pour $i = 1$, et donc $C_{i,i}(M) = C_{1,1}(M)$, c'est à dire $M = C_{1,1}(M)I_n \in \mathcal{H}^*(n,K)$.

Alors $\overline{M}$ est l'élément neutre de $\mathrm{PGL}(n,K)$, ce qui signifie que le centre de $\mathrm{PGL}(n,K)$ est l'élément neutre. Cette démonstration fonctionne aussi pour $\mathrm{PSL}(n,K)$, car les $T_{i,j}(\rho)$ et N_1 appartiennent à $\mathrm{SL}(n,K)$. □

2 Les groupes projectifs

Soit E un K-e.v. de dimension finie $n \in \mathbb{N}^*$. On note $\mathrm{GL}_K(E)$ le groupe linéaire de E, c'est-à-dire le groupe des automorphismes de E. $\mathrm{SL}_K(E)$ est le noyau du déterminant vu comme morphisme de groupes de $\mathrm{GL}_K(E)$ dans K^*.

Soit $\mathfrak{B}$ une base de E. L'application $\phi^{\mathfrak{B}} : u \to \mathrm{Mat}_{\mathfrak{B}}(u)$ est un isomorphisme entre $\mathrm{GL}_K(E)$ et $\mathrm{GL}(n,K)$, entre $\mathrm{SL}_K(E)$ et $\mathrm{SL}(n,K)$, entre $\mathcal{H}_K(E)$ et $\mathcal{H}(n,K)$, entre $\mathcal{H}_K^*(E)$ et $\mathcal{H}^*(n,K)$, et entre $\mathrm{S}\mathcal{H}_K^*(E)$ et $\mathrm{S}\mathcal{H}^*(n,K)$.

Soient alors $\mathrm{PGL}_K(E) = \mathrm{GL}_K(E)/\mathcal{H}_K^*(E)$ et $\mathrm{PSL}_K(E) = \mathrm{SL}_K(E)/\mathrm{S}\mathcal{H}_K^*(E)$; le morphisme $\phi^{\mathfrak{B}}$ induit naturellement un isomorphisme entre $\mathrm{PGL}_K(E)$ et $\mathrm{PGL}(n,K)$ et entre $\mathrm{PSL}_K(E)$ et $\mathrm{PSL}(n,K)$. Dans la suite, nous passerons du point de vue matriciel au point de vue vectoriel sans forcément préciser dans quelle base.

2.1 Propriétés élémentaires

En applicant le théorème 1.2 et le corollaire 1.2, on obtient :

Théorème 2.1. *On a :*
- $\mathcal{Z}_{\mathrm{GL}_K(E)}(\mathrm{SL}_K(E)) = \mathcal{H}_K^*(E)$, $C_{\mathrm{Hom}_K(E)}(\mathrm{SL}_K(E)) = \mathcal{H}_K(E)$;
- *le centre de* $\mathrm{GL}_K(E)$ *est* $\mathcal{H}_K^*(E)$, *le centre de* $\mathrm{SL}_K(E)$ *est* $\mathcal{SH}_K^*(E)$.

En applicant le corollaire 1.3, on a :

Théorème 2.2. *Les centres de* $\mathrm{PGL}_K(E)$ *et de* $\mathrm{PSL}_K(E)$ *sont réduits à l'élément neutre.*

On définit enfin K^{*n} l'image de K^* par l'endomorphisme $\lambda \to \lambda^n$. On cherche désormais à déterminer les relations entre les groupes précédemment définis. Commençons par les injections naturelles obtenues par inclusion : $\mathrm{S}\mathcal{H}_K^*(E) \subset \mathcal{H}_K^*(E) \subset \mathrm{GL}_K(E)$, et $\mathrm{S}\mathcal{H}_K^*(E) \subset \mathrm{SL}_K(E) \subset \mathrm{GL}_K(E)$. On obtient alors le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{S}\mathcal{H}_K^*(E) & \longrightarrow & \mathcal{H}_K^*(E) \\ \downarrow & & \downarrow \\ \mathrm{SL}_K(E) & \xrightarrow{j} & \mathrm{GL}_K(E) \end{array}$$

Soit désormais ψ la sujection canonique de $\mathrm{SL}_K(E)$ dans $\mathrm{PSL}_K(E)$ et ϕ la surjection de $\mathrm{GL}_K(E)$ dans $\mathrm{PGL}_K(E)$. Puisque $\mathrm{S}\mathcal{H}_K^*(E) \subset \mathcal{H}_K^*(E)$, l'injection j entre $\mathrm{SL}_K(E)$ et $\mathrm{GL}_K(E)$ induit une injection $\overline{j}$ entre $\mathrm{PSL}_K(E)$ et $\mathrm{PGL}_K(E)$, pour laquelle on a naturellement $\overline{j} \circ \psi = \phi \circ \overline{j}$. On a donc le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{SL}_K(E) & \xrightarrow{j} & \mathrm{GL}_K(E) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} \\ \mathrm{PSL}_K(E) & \xrightarrow{\overline{j}} & \mathrm{PGL}_K(E) \end{array}$$

Désormais, on considère l'application det restreinte à deux ensemble : $\det|_{\mathcal{H}_K^*(E)}$, surjective dans K^{*n}, et $\det|_{\mathrm{GL}_K(E)}$, surjective dans K^*. On a par inclusion de K^{*n} dans K^* le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{H}_K^*(E) & \xrightarrow{\det} & K^{*n} \\ \downarrow & & \downarrow \\ \mathrm{GL}_K(E) & \xrightarrow{\det} & K^* \end{array}$$

Enfin, soit $\overline{\omega}$ la surjection canonique de K^* dans K^*/K^{*n}, et $f = \overline{\omega} \circ \det|_{\mathrm{GL}_K(E)}$. f est surjective, et $\mathcal{H}_K^*(E) \subset \ker(f)$; on peut alors définir un morphisme δ : $\mathrm{PGL}_K(E) \to K^*/K^{*n}$ par $\delta(\phi(x)) = f(x)$, ce qui nous donne le diagramme suivant :

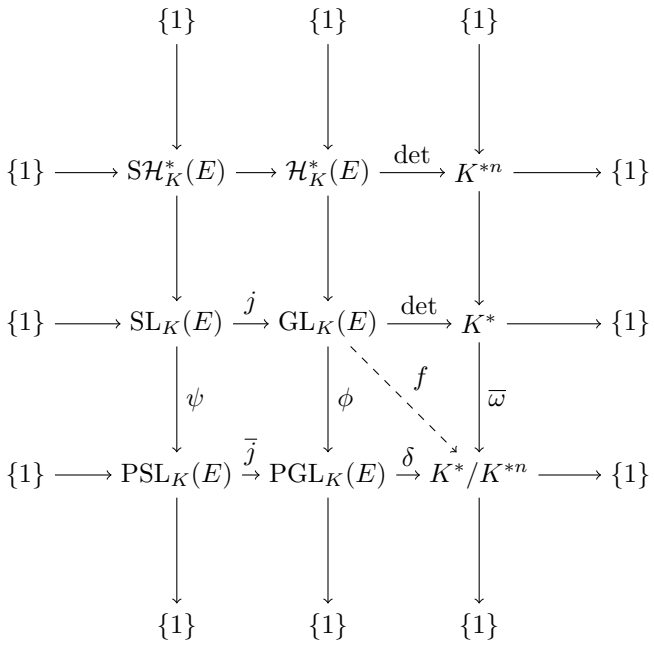
$$\begin{array}{ccc} \mathrm{GL}_K(E) & \xrightarrow{\det} & K^* \\ \downarrow{\scriptstyle \phi} & \searrow^{f} & \downarrow{\scriptstyle \overline{\omega}} \\ \mathrm{PGL}_K(E) & \xrightarrow{\delta} & K^*/K^{*n} \end{array}$$

On a de plus :
— $\ker(\det|_{\mathcal{H}_K^*(E)}) = \mathrm{S}\mathcal{H}_K^*(E)$;
— $\ker(\det|_{\mathrm{GL}_K(E)}) = \mathrm{SL}_K(E)$;
— δ est surjective car f l'est, et $\ker(\delta) = \mathrm{Im}(\overline{j})$, en effet :

1. Soit $x \in \mathrm{Im}(\overline{j})$, alors il existe $\overline{u} \in \mathrm{PSL}_K(E)$ tel que $x = \overline{j}(\overline{u})$. De plus, par surjectivité de ψ, il existe $u \in \mathrm{SL}_K(E)$ tel que $\overline{u} = \psi(u)$. On a par la commutativité précédemment établie $x = \overline{j} \circ \psi(u) = \phi \circ j(u) = \phi(u)$, d'où $\delta(x) = \delta \circ \phi(u) = f(u) = \overline{\omega}(det(u))$, or $u \in \mathrm{SL}_K(E)$, donc $\det(u) = 1_K$, c'est-à-dire $x \in \ker(\delta)$.

2. Soit $\overline{u} \in \ker(\delta)$. Par surjectivité de ϕ, il existe $u \in \mathrm{GL}_K(E)$ tel que $\phi(u) = \overline{u}$. On a de plus $\forall \lambda \in E\ \phi(\lambda \,\mathrm{id}_E) = \phi(id_E)$, donc $\phi(\lambda u) = \overline{u}$. On a $\delta(\overline{u}) = \delta \circ \phi(u) = \overline{\omega}(\det(u))$, donc comme $\overline{u} \in \ker(\delta)$, $\det(u) \in K^{*n}$, c'est-à-dire que $\det(u)$ s'écrit α^n avec $\alpha \in K^*$. Alors $v = \alpha^{-1}u \in \mathrm{SL}_K(E)$, et $\phi(v) = \overline{u}$; mais $\phi(v) = \phi \circ j(v) = \overline{j} \circ \psi(v)$, donc $\overline{u} \in \mathrm{Im}(\overline{j})$.

On peut résumer toutes ces informations dans le diagramme suivant :



C'est un diagramme commutatif et exact par lignes et par colonnes.

2.2 Simplicité

2.2.1 Transvections & dilatations

Les transvections de E sont définies comme les éléments τ de $\mathrm{GL}_K(E)$ pour lesquels il existe un hyperplan H de E, un élément v_0 non-nul de H, et une forme linéaire ϕ de noyau H tels que

$$\forall x \in E \quad \tau(x) = x + \phi(x)v_0$$

Alors $H = \ker(\tau - \mathrm{id}_E)$, on l'appelle *l'hyperplan de* τ.

Fixons $\phi \in E^*$ et soit $H = \ker(\phi)$, alors pour tout $v \in H$, on définit $\tau_{\phi,v} \in \mathrm{GL}_K(E)$ par :

$$\forall x \in E \quad \tau_{\phi,v}(x) = x + \phi(x)v$$

L'application $\tau_{\phi,\cdot} : H \to \mathrm{GL}_K(E)$, $v \to \tau_{\phi,v}$ est un morphisme injectif du groupe $(H,+)$ dans $\mathrm{GL}_K(E)$; son image est l'ensemble des transvections d'hyperplan H et l'identité.

Théorème 2.3. *$\tau \in \mathrm{GL}_K(E)$ est une transvection ssi il existe une base de E dans laquelle la matrice de τ est de transvection. Dans ce cas, il existe aussi une base de E dans laquelle cette matrice est $T_{1,2}(1)$.*
En particulier, toute transvection est dans $\mathrm{SL}_K(E)$.

Démonstration. Soit τ une transvection, H son hyperplan, ϕ une forme linéaire de noyau H et $v \in H$ non nul tels que $\tau(x) = x + \phi(x)v$ pour tout $x \in E$.

Par le théorème de la base incomplète, on forme une base de H contenant v. Cette base de H est une famille libre de E, on peut donc la compléter en une base de E à l'aide d'un élement e de E. On obtient donc la base suivante :

$$\mathfrak{B} = \{v, h_1, h_2, \ldots, h_{n-2}, e\} \quad h_i \in H$$

Alors $\tau(v) = v$, $\tau(h_i) = h_i$ car $\tau_H = \mathrm{id}_H$; et $\tau(e) = e + \phi(e)v$. Ainsi :

$$\mathrm{Mat}_{\mathfrak{B}}(\tau) = \left(\begin{array}{ccccc|c} & & & & & 0 \\ & & I_{n-1} & & & \vdots \\ & & & & & 0 \\ \hline \phi(e) & 0 & \cdots & 0 & & 1 \end{array}\right) = T_{n,1}(\phi(e))$$

On a donc démontré pour toute transvection τ l'existence d'une base dans laquelle la matrice de τ est une matrice de transvection.

Prenons désormais $\tau \in \mathrm{GL}_K(E)$ et $\mathfrak{B} = \{e_1, \ldots, e_n\}$ une base de E telle que $\mathrm{Mat}_{\mathfrak{B}}(\tau) = T_{i,j}(\lambda)$ de transvection. Alors pour $k \neq j$, $\tau(e_k) = e_k$ et $\tau(e_j) = e_j + \lambda e_i$. On note $H = \ker(\tau - \mathrm{id}_E) = \{e_k | k \neq j\}$, c'est un hyperplan de E. On définit ϕ la forme linéaire de E telle que $\phi(e_k) = 0$ pour $k \neq i$, et $\phi(e_i) = \lambda$. Alors $\ker(\phi) = H$, et $\forall x \in E$, $\tau(x) = x + \phi(x)e_i$, donc τ est une transvection.

On a ainsi l'équivalence. Montrons désormais que pour toute transvection de E, il existe une base de E dans laquelle la matrice de cette transvection est $T_{1,2}$.

Soit τ une transvection, et $\mathfrak{B} = \{e_1, \ldots, e_n\}$ une base de E telle que $\mathrm{Mat}_{(B}(\tau) = T_{i,j}(\lambda)$. Alors, on a pour $k \neq j$, $\tau(e_k) = e_k$ et $\tau(e_j) = e_j + \lambda e_i$. Posons pour $k \neq i$, $e'_k = e_k$, et $e'_i = \lambda e_i$. Alors $\tau(e'_k) = (e'_k)$ pour $k \neq j$, et $\tau(e'_j) = e'_j + e'_i$. Enfin, soit $\sigma \in \mathfrak{S}_n$ défini par $\sigma = (1\ i)(2\ j)$. Alors soit $\mathfrak{B}' = \{e'_{\sigma(1)}, \ldots, e'_{\sigma(n)}\}$, on a $\tau(e'_{\sigma(2)}) = e'_{\sigma(2)} + e'_{\sigma(1)}$ et $\tau(e'_{\sigma(k)}) = e'_{\sigma(k)}$ pour $k \neq 2$, c'est-à-dire $\mathrm{Mat}_{\mathfrak{B}'}(\tau) = T_{1,2}(1)$.

On constate enfin que le résultat précédent implique $\det(\tau) = \det(T_{1,2}(1)) = 1$, et donc que $\tau \in \mathrm{SL}_K(E)$. □

Par le théorème 1.1, on a immédiatement :

Corollaire 2.1. $\mathrm{SL}_K(E)$ *est engendré par l'ensemble des transvections de* E.

De plus, comme toutes les matrices de transvection sont conjuguées à $T_{1,2}(1)$ dans $\mathrm{GL}(n, K)$, on obtient :

Corollaire 2.2. *Deux transvections de* E *sont conjuguées dans* $\mathrm{GL}_K(E)$*, et toute conjuguée d'une transvection de* E *est une transvection.*

Nous pouvons désormais démontrer le théorème suivant :

Théorème 2.4. *Soit* H *un hyperplan de* E *et* $\tau \in \mathrm{Hom}_K(E)$*. Si* $\tau \neq \mathrm{id}_E$*,* $H \subset \ker(\tau - \mathrm{id}_E)$*, et* $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H$ *; alors* τ *est une transvection de* E *d'hyperplan* H*.*

Démonstration. Soit $x_0 \in E \backslash H$, alors $E = H \oplus K \cdot x_0$, et donc $H \subset \ker(\tau - \mathrm{id}_E) \Rightarrow \ker(\tau - \mathrm{id}_E) = H$ ou E. Mais $\tau \neq \mathrm{id}_E$, donc $\ker(\tau - \mathrm{id}_E) = H$.
Posons $v_0 = \tau(x_0) - x_0$. $v_0 \neq 0_E$ car $x_0 \notin \ker(\tau - \mathrm{id}_E) = H$, et $v_0 \in \mathrm{Im}(\tau - id_E) \subset H$. Soit ϕ la forme linéaire de noyau H telle que $\phi(x_0) = 1$, on pose $\tau' = \tau_{\phi, v_0}$. Alors pour $x \in H$, $\tau(x) - \tau'(x) = x - x = 0_E$, et $\tau(x_0) - \tau'(x_0) = v_0 + x_0 - (x_0 + \phi(x_0)v_0) = 0_E$.
Ainsi $\tau = \tau'$, ce qui signifie que τ est une transvection. □

Pour H un hyperplan de E, on appelle *dilatation d'hyperplan* H tout élément $\delta \in \mathrm{GL}_K(E)$ pour lequel il existe D une droite supplémentaire de H dans E et $\rho \in K^*$ tels que $\delta|_H = \mathrm{id}_H$ et $\delta|_D = \rho \cdot \mathrm{id}_D$. ρ est appelé *le rapport de* δ. Si $\rho \neq 1_K$, $H = \ker(\delta - \mathrm{id}_E)$ est appelé *l'hyperplan de* δ. Si $\rho = 1_K$, $\delta = \mathrm{id}_E$.

On a facilement l'équivalence entre $\delta \in \mathrm{GL}_K(E)$ est une transvection de rapport ρ et l'existence d'une base de E dans laquelle la matrice de δ est $D(\rho)$. cela signifie que deux transvections sont conjuguées dans $\mathrm{GL}_K(E)$ ssi elles ont le même rapport.
Le théorème 1.1 donne :

Théorème 2.5. $\mathrm{GL}_K(E)$ *est engendré par l'ensemble des dilatations et des transvections.*

Soit H un hyperplan de E. On définit $\Gamma_H = \{u \in \mathrm{GL}_K(E) | H \subset \ker(u - \mathrm{id}_E)\}$, c'est un sous-groupe de $\mathrm{GL}_K(E)$. L'application $\delta_H : \Gamma_H \to K^*$, $u \to \det(u)$ est un morphisme de groupes.

Théorème 2.6. *L'application* δ_H *est surjective,* $\ker(\delta_H)$ *est l'ensemble des transvections d'hyperplan* H *et de l'identité, et* $\Gamma_H \backslash \ker(\delta_H)$ *est l'ensemble des dilatations d'hyperplan* H *et de rapport* $\neq 1_K$*.*

Démonstration. Toute dilatation d'hyperplan H appartient à Γ_H, ce qui implique que δ_H est surjective. On sait aussi que toute transvection d'hyperplan H appartient à Γ_H, et comme le déterminant d'une transvection est toujours 1_K, toute transvection d'hyperplan H appartient à $\ker(\delta_H)$.

Soit $u \in \Gamma_H \backslash \ker(\delta_H)$, on notera $\lambda = \delta_H(u) = \det(u)$. Fixons une base $\mathfrak{B} = \{e_1, \dots, e_n\}$ de E telle que $\{e_1, \dots, e_{n-1}\}$ soit une base de H. Alors :

$$\mathrm{Mat}_{\mathfrak{B}}(u) = \left(\begin{array}{ccc|c} & I_{n-1} & & X \\ \hline 0 & \dots & 0 & \lambda \end{array}\right)$$

avec $X \in \mathfrak{M}_{n-1,1}$. Si $X = 0$, on a démontré que u est une dilatation ; sinon, on pose $x_n = u(e_n) - e_n$. On a $x_n \notin H$ car $\lambda \neq 1_K$, et $x_n \neq 0_E$, donc $\mathfrak{B}' = \{e_1, \dots, e_{n-1}, x_n\}$ est une base de E. De plus, en notant $u(e_n) = \lambda e_n + x$ avec $x \in H$, on obtient $u(x_n) = u(\lambda e_n + x - e_n) = (\lambda - 1)u(e_n) + x = (\lambda - 1)(\lambda e_n + x) + x = \lambda((\lambda - 1)e_n + x) = \lambda(u(e_n) - e_n) = \lambda x_n$, donc $\mathrm{Mat}_{\mathfrak{B}'}(u) = D(\lambda)$ et u est une dilatation.

Soit désormais $\tau \in \ker(\delta_H)$ avec $\tau \neq \mathrm{id}_E$, alors dans la base $\mathfrak{B}$ précédemment définie :

$$\mathrm{Mat}_{\mathfrak{B}}(u) = \left(\begin{array}{ccc|c} & I_{n-1} & & X \\ \hline 0 & \dots & 0 & 1 \end{array}\right)$$

Ceci implique immédiatement $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H$, et donc d'après le théorème 2.4, τ est une transvection. □

On a alors $\ker(\delta_H) \triangleleft \Gamma_H$, et $\Gamma_H / \ker(\delta_H) \cong K^*$.

Théorème 2.7. *Pour $n \geqslant 3$, deux transvections de E sont conjuguées dans $\mathrm{SL}_K(E)$.*

Démonstration. Soit τ et τ' deux transvection, $\mathfrak{B} = \{e_1, \dots, e_n\}$ et $\mathfrak{B}' = \{e'_1, \dots, e'_n\}$ deux bases de E telles que $\mathrm{Mat}_{\mathfrak{B}}(\tau) = \mathrm{Mat}_{\mathfrak{B}'}(\tau') = T_{2,1}(1)$. Alors pour $\rho \in K^*$, on définit $u_\rho \in \mathrm{GL}_K(E)$ telle que $u_\rho(e_i) = e'_i$ pour $i \neq n$, et $u_\rho(e_n) = \rho(e'_n)$. Puisque $n \geqslant 3$, e_n est distinct de e_1 et e_2, et donc $u_\rho \tau u_\rho^{-1} = \tau'$. D'autre part, $\det(u_\rho) = \rho \det(u_{1_K})$, donc $\det(u_{(\det(u_{1_k}))^{-1}}) = 1_K$, ce qui signifie $u_{(\det(u_{1_k}))^{-1}} \in \mathrm{SL}_K(E)$, et donc τ et τ' sont conjuguées dans $\mathrm{SL}_K(E)$. □

Théorème 2.8. *Fixons $n = 2$.*
Soit $\mathcal{C}_T$ l'ensemble des classes de conjugaison par $\mathrm{SL}_K(E)$ des transvections de E. Il y une bijection naturelle entre le groupe quotient K^*/K^{*2} et $\mathcal{C}_T$. Précisément, soit C une transversale dans K^*/K^{*2} ; alors l'ensemble $\mathcal{E}_C$ des matrices $T_{1,2}(\rho)$ où ρ parcourt C est une transversale de $\mathcal{C}_T$ dans $\mathrm{SL}_K(E)$.

Démonstration. Posons $T_\rho = T_{1,2}(\rho)$, alors pour ρ et ρ' dans K^*, il nous suffit de prouver que T_ρ et $T_{\rho'}$ sont conjuguées dans $\mathrm{SL}_K(E)$ ssi $\rho'/\rho \in K^{*2}$.
Si il existe a tel que $\rho = a^2\rho'$, alors $T_{\rho'} = \mathrm{Diag}(a, a^{-1}) \times T_\rho \times \mathrm{Diag}(a^{-1}, a)$;
Et si il existe $P = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, K)$ telle que $T_{\rho'} = P \times T_\rho \times P^{-1}$, alors le calcul nous donne $\rho' = a^2\rho$. □

2.2.2 Commutateurs

Pour G un groupe multiplicatif, *le groupe des commutateurs* de G, noté $[G,G]$, est le groupe engendré par les éléments $[x,y] = xyx^{-1}y^{-1}$, $x,y \in G$. On a :

$[G,G] \triangleleft G$ **:** soit $z = xyx^{-1}y^{-1} \in [G,G]$, et $g \in G$, alors :

$$gzg^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in [G,G]\,.$$

$G/[G,G]$ **abélien :** pour $x,y \in G$, on a : $xyx^{-1}y^{-1} \in [G,G]$, alors si l'on note pour $\overline{z}$ la classe d'équivalence de $z \in G$ dans $G/[G,G]$, on a :

$$\overline{xyx^{-1}y^{-1}} = \overline{1_G} \Rightarrow \overline{xy} = \overline{yx}.$$

$H \triangleleft G$ **et** G/H **abélien** $\Rightarrow H \supset [G,G]$ **:** Soient $x,y \in G$, alors dans G/H, $\overline{xy} = \overline{yx}$, donc $\overline{xyx^{-1}y^{-1}} = \overline{1_G}$, ou encore $xyx^{-1}y^{-1} \in H$.

Dans le cadre notre étude, nous allons déterminer les commutateurs de $\mathrm{GL}_K(E)$ et $\mathrm{SL}_K(E)$:

Théorème 2.9. *Hormis dans les cas* $(n=2, K=\mathbb{F}_2)$ *et* $(n=2, K=\mathbb{F}_3)$*, on a* $[\mathrm{GL}_K(E), \mathrm{GL}_K(E)] = [\mathrm{SL}_K(E), \mathrm{SL}_K(E)] = \mathrm{SL}_K(E)$.

Démonstration. Soient $M, N \in \mathrm{GL}_K(E)$, alors $\det(M \times N \times M^{-1} \times N^{-1}) = \det(M)\det(N)\det(M)^{-1}\det(N)^{-1} = 1_K$, donc $[\mathrm{GL}_K(E), \mathrm{GL}_K(E)] \subset \mathrm{SL}_K(E)$.

1. si $n = 1$, le résultat est trivial.
2. si $n \geqslant 3$, on fixe un hyperplan H, ϕ une forme linéaire de noyau H, et $v_0 \in H$ non nul ; on note $\tau = \tau_{\phi,v_0}$ la transvection associée. On a $\tau^{-1} = \tau_{\phi,-v_0}$. On chosit v_0' dans H, non nul, et distinct de v_0 et $-v_0$; c'est possible car $|H| = |K|^{n-1}$, or $|K| \geqslant 2$ et $n-1 \geqslant 2 \Rightarrow |H| \geqslant 4$. On pose $\tau' = \tau_{\phi,v_0'}$, alors $\tau' \neq \tau$, $\tau' \neq \tau^{-1}$; puisque τ et τ' sont deux transvections d'hyperplan H, et que $\tau\tau' \neq \mathrm{id}_E$, le théorème 2.6 nous dit que $\tau\tau'$ est une transvection. Le théorème 2.7 nous donne l'existence de $u \in \mathrm{SL}_K(E)$ tel que $\tau\tau' = u\tau' u^{-1}$, ou encore $\tau = u\tau u^{-1}\tau^{-1} \in [\mathrm{SL}_K(E), \mathrm{SL}_K(E)]$. Ainsi $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)]$ contient toutes les transvections, et donc contient $\mathrm{SL}_K(E)$, et $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)]$ est naturellement inclus dans $\mathrm{SL}_K(E)$, donc $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)] = \mathrm{SL}_K(E)$.
   Enfin, $\mathrm{SL}_K(E) \subset \mathrm{GL}_K(E) \Rightarrow [\mathrm{SL}_K(E), \mathrm{SL}_K(E)] \subset [\mathrm{GL}_K(E), \mathrm{GL}_K(E)]$, donc $[\mathrm{GL}_K(E), \mathrm{GL}_K(E)] = \mathrm{SL}_K(E)$.
3. si $n = 2$, nous raisonnerons sur $\mathrm{SL}(2,K)$ pour des raisons pratiques.
   Pour $\lambda \in K$ et $a \in K^*$, on pose $T(\lambda) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, et $\Delta(a) = \mathrm{Diag}(a, a^{-1})$. On a alors $T(\lambda) \times \Delta(a) \times T(\lambda)^{-1} \times \Delta(a)^{-1} = T(\lambda) \times \Delta(a) \times T(-\lambda) \times \Delta(a^{-1}) = \begin{pmatrix} 1 & \lambda(1-a^2) \\ 0 & 1 \end{pmatrix} = T(\lambda(1-a^2))$.
   Les hypothèses nous donnent $|K| \geqslant 4$, et l'on peut alors choisir $a \in K^*$ tel que $a^2 \neq 1_K$. En faisant varier λ et en applicant le même raisonnement à ${}^tT(\lambda)$, on constate que $[\mathrm{SL}(2,K), \mathrm{SL}(2,K)]$ contient toutes les matrices de transvection, et donc que $[\mathrm{SL}(2,K), \mathrm{SL}(2,K)] \subset \mathrm{SL}(2,K)$. Le reste de la preuve se déroule comme pour $n \geqslant 3$.

□

Regardons de plus près les cas exclus par le théorème :

$n = 2$, $K = \mathbb{F}_2$ Pour $M \in \mathfrak{M}_2(K)$, $\det(M) \neq 0 \Leftrightarrow \det(M) = 1$. Donc $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2)$, et par ailleurs $\mathcal{H}^*(2,\mathbb{F}_2) = \mathrm{S}\mathcal{H}^*(2,\mathbb{F}_2) = \{I_2\}$, donc $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{PGL}(2,\mathbb{F}_2) = \mathrm{PSL}(2,\mathbb{F}_2)$. $\mathrm{GL}(2,\mathbb{F}_2)$ agit naturellement sur $K^2\backslash\{(0_K,0_K)\}$ qui est de cardinal 3 ; $\mathrm{GL}(2,\mathbb{F}_2)$ peut donc être vu comme un sous-groupe de $\mathfrak{S}_3$. Mais $|\mathrm{GL}(2,\mathbb{F}_2)| = 6 = |\mathfrak{S}_3|$, donc $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) \cong \mathfrak{S}_3$. Or $[\mathfrak{S}_3,\mathfrak{S}_3] = \mathfrak{A}_3$.

$n = 2$, $K = \mathbb{F}_3$ On a la suite exacte :

$$\{1\} \to \mathrm{SL}(2,\mathbb{F}_3) \to \mathrm{GL}(2,\mathbb{F}_3) \to \mathbb{F}_3^* \to \{1\}$$

Comme $|\mathbb{F}_3^*| = 2$, $\mathrm{SL}(2,\mathbb{F}_3)$ est d'indice 2 dans $\mathrm{GL}(2,\mathbb{F}_3)$. On a par dénombrement $|\mathrm{GL}(2,\mathbb{F}_3)| = 48$, $|\mathrm{SL}(2,\mathbb{F}_3)| = 24$. Faisons opérer $\mathrm{SL}(2,\mathbb{F}_3)$ sur l'ensemble $\mathcal{D}$ des 4 droites vectorielles de K^2 : cette action correspond à un morphisme $\phi : \mathrm{SL}(2,\mathbb{F}_3) \to \mathfrak{S}_\mathcal{D} \cong \mathfrak{S}_4$, de noyau $\mathcal{H}^*(2,\mathbb{F}_3) = \{I_2,-I_2\}$, ainsi $\mathrm{SL}(2,\mathbb{F}_3)/\ker(\phi) \cong \mathrm{Im}(\phi) \Rightarrow |\mathrm{Im}(\phi)| = 12$. Or le seul sous-groupe de $\mathfrak{S}_4$ de cardinal 12 est $\mathfrak{A}_4$.

Soit $\mathcal{K}$ le groupe composé des bitranspositions de $\mathfrak{A}_4$ et de l'identité. Alors :
- Soit $(x\,y)(w\,z) \in \mathcal{K}$, alors $\sigma = (x\,w\,z)$ et $\tau = (x\,y\,z)$ sont tels que $\sigma\tau\sigma^{-1}\tau^{-1} = (x\,y)(w\,z)$, donc $\mathcal{K} \subset [\mathfrak{A}_4,\mathfrak{A}_4]$.
- Soit $\tau \in \mathcal{K}$ et $\sigma \in \mathfrak{A}_4$, alors $(\sigma\tau\sigma^{-1})^2 = \sigma\tau^2\sigma^{-1} = \sigma\,\mathrm{id}\,\sigma^{-1} = \mathrm{id}$, c'est-à-dire $\sigma\tau\sigma^{-1}$ est d'ordre $\leqslant 2$, et donc appartient à $\mathcal{K}$, ce qui donne $\mathcal{K} \triangleleft \mathfrak{A}_4$.
- $|\mathfrak{A}_4/\mathcal{K}| = \frac{12}{4} = 3$, donc $\mathfrak{A}_4/\mathcal{K} \cong \mathfrak{A}_3$ est abélien ; ainsi $\mathcal{K} \supset [\mathfrak{A}_4,\mathfrak{A}_4]$.

Le morphisme ϕ induit un morphisme ψ entre $\mathrm{SL}(n,\mathbb{F}_3)/[\mathrm{SL}(n,\mathbb{F}_3),\mathrm{SL}(n,\mathbb{F}_3)]$ et $\mathfrak{A}_4/[\mathfrak{A}_4,\mathfrak{A}_4]$; en effet, si l'on note π la surjection canonique de $\mathrm{SL}(n,\mathbb{F}_3)$ dans $\mathrm{SL}(n,\mathbb{F}_3)/[\mathrm{SL}(n,\mathbb{F}_3),\mathrm{SL}(n,\mathbb{F}_3)]$ et κ la surjection de $\mathfrak{A}_4$ dans $\mathfrak{A}_4/[\mathfrak{A}_4,\mathfrak{A}_4]$, alors on définit ψ tel que $\forall M \in \mathrm{SL}(2,\mathbb{F}_3)$, $\psi(\pi(M)) = \kappa(\phi(M))$. Alors :
- ψ est bien définie car si M et N dans $\mathrm{SL}(2,\mathbb{F}_3)$ sont telles que $\pi(M) = \pi(N)$, alors il existe P et Q dans $\mathrm{SL}(2,\mathbb{F}_3)$ telles que $M = N \times P \times Q \times P^{-1} \times Q^{-1}$, d'où $\phi(M) = \phi(N)\phi(P)\phi(Q)\phi(P)^{-1}\phi(Q)^{-1}$, ce qui donne $\kappa(\phi(M)) = \kappa(\phi(N))$, ou encore $\psi(\pi(M)) = \psi(\pi(N))$.
- ψ est surjective car κ et ϕ sont surjectives.
- ψ est injective car si $M \in \mathrm{SL}(2,\mathbb{F}_3)$ est telle que $\psi(\pi(M)) = 1_{\mathfrak{A}_4/[\mathfrak{A}_4,\mathfrak{A}_4]}$, alors $\kappa(\phi(M)) = 1_{\mathfrak{A}_4/[\mathfrak{A}_4,\mathfrak{A}_4]}$, ce qui signifie $\phi(M) \in [\mathfrak{A}_4,\mathfrak{A}_4]$. Donc, $\phi(M) = \sigma\tau\sigma^{-1}\tau^{-1}$, avec $\sigma,\tau \in \mathfrak{A}_4$. Par surjectivité de ϕ, il existe P et Q dans $\mathrm{SL}(2,\mathbb{F}_3)$ telles que $\phi(P) = \sigma$, et $\phi(Q) = \tau$. Alors $\phi(M) = \phi(P \times Q \times P^{-1} \times Q^{-1})$, c'est à dire $M \times Q \times P \times Q^{-1} \times P^{-1} \in \ker(\phi)$. Or, $\ker(\phi) \subset [\mathrm{SL}(2,\mathbb{F}_3),\mathrm{SL}(2,\mathbb{F}_3)]$; en effet, soit $J = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, alors en notant $U = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $V = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, on a $J = U \times V \times U^{-1} \times V^{-1}$, donc $J \in [\mathrm{SL}(2,\mathbb{F}_3),\mathrm{SL}(2,\mathbb{F}_3)]$; et $J^2 = -I_2$. D'où $M \in [\mathrm{SL}(2,\mathbb{F}_3),\mathrm{SL}(2,\mathbb{F}_3)]$, donc $\pi(M) = 1_{\mathrm{SL}(n,\mathbb{F}_3)/[\mathrm{SL}(n,\mathbb{F}_3),\mathrm{SL}(n,\mathbb{F}_3)]}$.

Donc $\mathrm{SL}(n,\mathbb{F}_3)/\left[\mathrm{SL}(n,\mathbb{F}_3),\mathrm{SL}(n,\mathbb{F}_3)\right] \cong \mathfrak{A}_4/\left[\mathfrak{A}_4,\mathfrak{A}_4\right] \cong \mathfrak{A}_3$, et le théorème est mis en défaut car $\left[\mathrm{SL}(n,\mathbb{F}_3),\mathrm{SL}(n,\mathbb{F}_3)\right] = \{I_2,-I_2,J,-J\} \neq \mathrm{SL}(n,\mathbb{F}_3)$. Si l'on applique le même raisonnement à $\mathrm{GL}(2,\mathbb{F}_3)$, on trouve en revanche $\left[\mathrm{GL}(2,\mathbb{F}_3),\mathrm{GL}(2,\mathbb{F}_3)\right] = \mathrm{SL}(2,\mathbb{F}_3)$, ce qui est conforme au théorème.

2.2.3 Démonstration de la simplicité

On supposera $n \geqslant 2$, et on posera $\mathcal{Z} = \mathrm{S}\mathcal{H}_K^*(E)$. On sait que $\mathcal{Z}$ est isomorphe à $\{\xi \in K^* \mid \xi^n = 1_K\}$, qui est un sous-groupe fini de K^*.

Théorème 2.10. *Hormis dans les cas $(n=2, K=\mathbb{F}_2)$ et $(n=2, K=\mathbb{F}_3)$, le groupe $\mathrm{PSL}_K(E)$ est simple et non-abélien.*

Démonstration. On montrera une propriété plus forte, qui implique le théorème 2.10 : Si G est un sous-groupe distingué de $\mathrm{SL}_K(E)$, alors on a $G \subset \mathcal{Z}$ ou $G = \mathrm{SL}_K(E)$. Ceci implique la smiplicité de $\mathrm{PSL}_K(E) = \mathrm{SL}_K(E)/\mathcal{Z}$; en effet, soit $H \triangleleft \mathrm{PSL}_K(E)$, et soit π la projection canonique de $\mathrm{SL}_K(E)$ dans $\mathrm{PSL}_K(E)$. Alors $G = \pi^{-1}(H)$ est distingué dans $\mathrm{SL}_K(E)$. Ainsi, si la propriété est vraie, on a soit $G = \mathrm{SL}_K(E)$ et $H = \mathrm{PSL}_K(E)$, soit $G \subset \mathcal{Z}$ et $H = \{1_{\mathrm{PSL}_K(E)}\}$.
Soit $G \triangleleft \mathrm{SL}_K(E)$ avec $G \not\subset \mathcal{Z}$. Si l'on note $\mathcal{G}_1(E)$ l'ensemble des droites vectorielles de E, alors $\mathcal{Z}$ est l'ensemble des $u \in \mathrm{SL}_K(E)$ laissant invariante chaque $D \in \mathcal{G}_1(E)$. Comme $G \not\subset \mathcal{Z}$, il existe $u_0 \in G$ et $D_1, D_2 \in \mathcal{G}_1(E)$ tels que $u_0(D_1) = D_2 \neq D_1$.

(a) Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$,
et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. Ce sont des sous-groupes de $\mathrm{SL}_K(E)$, et on a $\Gamma_D \subset \Phi_D$. Fixons $v \in D \backslash \{0_E\}$; pour $\phi \in E^*$, on note $\tau_{\phi,v}$ l'endomorphisme de E défini par $\tau_{phi,v}(x) = x + \phi(x)v$. Soit $\mathbb{F}_D = \{\psi \in E^* \mid \psi(D) = \{0_E\}\}$ l'orthogonal de D dans E^*. On a $\tau_{phi,v} \in \Gamma_D \Leftrightarrow \phi \in \mathbb{F}_D$. L'application $\mathbb{F}_D \to \Gamma_D$, $\phi \to \tau_{\phi,v}$ est un isomorphisme de groupes. Comme $(\mathbb{F}_D, +)$ est abélien, $(\Gamma_D, \circ)$ est donc abélien.

(b) Fixons $D_0 \in \mathcal{G}_1(E)$ et $\alpha \in \mathrm{SL}_K(E)$. On a $\Phi_{\alpha(D_0)} = \alpha\Phi_D\alpha^{-1}$ et $\Gamma_{\alpha(D_0)} = \alpha\Gamma_D\alpha^{-1}$. Puisque $\mathrm{SL}_K(E)$ est transitif sur $\mathcal{G}_1(E)$, les Φ_D et les Γ_D, où D parcourt $\mathcal{G}_1(E)$, sont tous conjugués dans $\mathrm{SL}_K(E)$.

(c) Montrons que l'action de G sur $\mathcal{G}_1(E)$ est transitive. Pour ce faire, prenons D_1' et $D_2' \in \mathcal{G}_1(E)$ distinctes. Alors choisissons $\alpha \in \mathrm{SL}_K(E)$ tel que $\alpha(D_1) = D_1'$ et $\alpha(D_2) = D_2'$, ce qui est possible car $n \geqslant 2$. Alors $\alpha u_0 \alpha^{-1} \in G$ car G est distingué dans $\mathrm{SL}_K(E)$, et $\alpha u_0 \alpha^{-1}(D_1') = D_2'$, ce qui nous donne la transitivité de G.
On a notamment $G\Phi_{D_0} = \Phi_{D_0}G = \mathrm{SL}_K(E)$; en effet, soit $\alpha \in \mathrm{SL}_K(E)$, alors il existe $u \in G$ tel que $u(D_0) = \alpha(D_0)$. On a donc $u^{-1}\alpha \in \Phi_{D_0}$, ce qui donne $\alpha \in u\Phi_{D_0} \subset G\Phi_{D_0}$. L'égalité $G\Phi_{D_0} = \Phi_{D_0}G$ est une conséquence du fait que G est distingué dans $\mathrm{SL}_K(E)$.

(d) Montrons que $G = \mathrm{SL}_K(E)$. Puisque $G \triangleleft \mathrm{SL}_K(E)$, $H = G\Gamma_{D_0} = \Gamma_{D_0}G$ est un sous-groupe de $\mathrm{SL}_K(E)$. Soit $\alpha \in \mathrm{SL}_K(E)$, d'après le théorème 2.1, $\alpha = \tau_1' \ldots \tau_r'$, avec $r \in \mathbb{N}^*$, et où les τ_i' sont des transvections. On définit

$D'_i = \mathrm{Im}(\tau'_i - \mathrm{id}_E)$, c'est une droite de E. Par transitivité de G sur $\mathcal{G}_1(E)$, il existe $u_i \in G$ tel que $u_i(D'_i) = D_0$. Posons alors $\tau_i = u_i t a u'_i u_i^{-1} : \tau_i \in \Gamma_{D_0}$. On en déduit $\alpha = (u_1^{-1}\tau_1 u_1)\dots(u_n^{-1}\tau_n u_n) \in H$, donc $H = \mathrm{SL}_K(E)$.
Ainsi $\mathrm{SL}_K(E)/G = G\Gamma_{D_0}/G \cong \Gamma_{D_0}/\Gamma_{D_0} \cap G$ par le deuxième théorème d'isomorphisme de Noether. Ainsi, $\mathrm{SL}_K(E)$ est abélien puisque Γ_{D_0} est abélien. On a alors $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)] \subset G$; grâce au théorème 2.9, on conclut que $G = \mathrm{SL}_K(E)$.

(e) Pour terminer la démonstration, il nous faut montrer que $\mathrm{PSL}_K(E)$ est non abélien. Nous allons exhiber un contre-exemple. Soit $U_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $V_2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, et $W_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Pour $n \geqslant 3$, on pose :

$$U_n = \left(\begin{array}{c|c} U_2 & 0 \\ \hline 0 & I_{n-2} \end{array}\right), V_n = \left(\begin{array}{c|c} V_2 & 0 \\ \hline 0 & I_{n-2} \end{array}\right), \text{ et } W_n = \left(\begin{array}{c|c} W_2 & 0 \\ \hline 0 & I_{n-2} \end{array}\right).$$

On vérifie alors que $U_n \times V_n \times U_n^{-1} \times V_n^{-1} = W_n$, or $W_n \notin \mathrm{S}\mathcal{H}^*(n, K)$. En notant $\overline{U_n}$ et $\overline{V_n}$ les classes d'équivalences de U_n et V_n dans $\mathrm{PSL}(n, K)$, on obtient $\overline{U_n}\,\overline{V_n} \neq \overline{V_n}\,\overline{U_n}$.

□

2.3 Cas d'un corps fini

On se place désormais dans le cas où $K = \mathbb{F}_q$, l'unique corps à q éléments. Dans ce cas, K^* est cyclique ; en effet, soit $d \in \mathbb{N}$ tel que $d|q-1$, alors s'il existe $x \in \mathbb{F}_q^*$ d'ordre d, on note $H =< x > \cong \mathbb{Z}/d\mathbb{Z}$. $|H| = d$, et pour tout $y \in H$, $y^d = 1$. De plus, le polynôme $X^d - 1$ a au plus d racines dans $\mathbb{F}_q$; ce qui signifie que l'ensemble des racines est exactement H. Ainsi l'ensemble des éléments d'ordre d dans $\mathbb{F}_q^*$, s'il en existe au moins 1, est l'ensemble des générateurs de H, au nombre de $\varphi(d)$, où φ est l'indicatrice d'Euler. En notant $N(d)$ le nombre d'éléments d'ordre d dans $\mathbb{F}_q^*$, on a $N(d) = 0$ ou $\varphi(d)$. Or, on a d'une part $q - 1 = \sum_{d|q-1} \varphi(d)$ grâce aux propriétés de φ, et d'autre part $q - 1 = \sum_{d|q-1} N(d)$ car l'ordre d'un élément d'un groupe fini divise le cardinal du groupe. Ainsi $N(d) = \varphi(d)$ pour $d|q-1$, et notamment $N(q-1) = \varphi(q-1) \neq 0$: il existe au moins un élément d'ordre $q-1$, qui engendre donc $\mathbb{F}_q^*$.

Pour $n \geqslant 2$ fixé, le cardinal de $\mathrm{GL}(n, \mathbb{F}_q)$ est le nombre de façon de choisir une matrice de rang n dans $\mathfrak{M}_n(\mathbb{F}_q)$, c'est-à-dire de choisir un n-uplet libre $(V_1, \dots, V_n)$ de vecteurs de $\mathbb{F}_q^n$. V_1 est non-nul, il y a donc $q^n - 1$ choix pour V_1. $V_2 \notin \mathrm{Vect}(V_1)$, il y a donc $q^n - q$ choix pour V_2. Pour i fixé, il y a $q^n - q^{i-1}$ choix pour V_i ; on obtient donc :

$$|\,\mathrm{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = \mathcal{E}(n, q)$$

On a $\mathcal{H}^*(n, \mathbb{F}_q) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$, donc $|\mathcal{H}^*(n, \mathbb{F}_q)| = |\mathbb{F}_q^*| = q-1$. Par ailleurs, $\mathrm{GL}(n, \mathbb{F}_q)/\,\mathrm{SL}(n, \mathbb{F}_q) \cong \{D(\lambda) | \lambda \in \mathbb{F}_q^*\} \cong \mathbb{F}_q^*$ par le théorème 1.1. Ainsi :

$$|\,\mathrm{PGL}(n, \mathbb{F}_q)| = |\,\mathrm{SL}(n, \mathbb{F}_q)| = \frac{\mathcal{E}(n, q)}{(q-1)}$$

Soit $\mathcal{Z}_n = \{\xi \in \mathbb{F}_q \mid \xi^n = 1_{\mathbb{F}_q}\}$. Puisque $\mathbb{F}_q^*$ est un groupe cyclique, il existe $\omega \in \mathbb{F}_q^*$ un générateur de $\mathbb{F}_q^*$. Déterminons l'ordre de ω^n : Soit $k \in \mathbb{N}^*$ tel que $(\omega^n)^k = 1$, alors il existe $a \in \mathbb{N}^*$ tel quel $nk = a(q-1)$. Le plus petit k pour lequel on a cette égalité est par définition $\frac{\text{ppcm}(n,q-1)}{n}$, or $\text{ppcm}(n, q-1) = \frac{n(q-1)}{\text{pgcd}(n,q-1)}$. Donc, en notant $d = \text{pgcd}(n, q-1)$ l'ordre de ω^n est $e = \frac{q-1}{d}$, et pour $k \in \mathbb{Z}$, $\omega^{nk} = 1_{\mathbb{F}_q} \Leftrightarrow k \equiv 0 \pmod{e}$. Soit désormais $\xi \in \mathbb{F}_q^*$, alors il existe $k \in \mathbb{Z}$ tel que $\omega^k = \xi$. Ainsi, $\xi \in \mathcal{Z}_n \Leftrightarrow \omega^{kn} = 1_{\mathbb{F}_q}$, et donc $\mathcal{Z}_n$ est le sous-groupe de $\mathbb{F}_q^*$ engendré par ω^e, qui est d'ordre d ; donc $\mathcal{Z}_n$ est un groupe cyclique d'ordre d. On sait par ailleurs que $\mathcal{Z}_n \cong \mathrm{S}\mathcal{H}^*(n, \mathbb{F}_q)$, donc :

$$|\operatorname{PSL}(n, \mathbb{F}_q)| = \frac{|\operatorname{SL}(n, \mathbb{F}_q)|}{|\mathrm{S}\mathcal{H}^*(n, \mathbb{F}_q)|} = \frac{\mathcal{E}(n,q)}{d(q-1)}$$

Nous avions précédemment établi $\operatorname{PSL}(2, \mathbb{F}_2) \cong \mathfrak{S}_3$ et $\operatorname{PSL}(2, \mathbb{F}_3) \cong \mathfrak{A}_4$, ici on retrouve $|\operatorname{PSL}(2, \mathbb{F}_2)| = 6$ et $|\operatorname{PSL}(2, \mathbb{F}_3)| = 12$. On remarque aussi que ces deux groupes ne sont pas simples, il est donc bien nécessaire de les exclure du théorème 2.10.

3 Le groupe simple d'ordre 168

On a d'après la formule précédente :

$$|\operatorname{PSL}(2, \mathbb{F}_7)| = |\operatorname{PSL}(3, \mathbb{F}_2)| = 168$$

Nous allons prouver que ces groupes sont isomorphes en montrant qu'il existe une seule structure de groupe simple à 168 éléments.

3.1 Le plan projectif à 7 points

Nous appelerons $\mathcal{S}_3$-système tout ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes, appelées conditions de $(1,2)$-incidence :

(I) Soient D_1 et $D_2 \in \mathcal{D}$ distincts, alors $D_1 \cap D_2$ est un singleton.

(II) Soient A_1 et $A_2 \in S$ distincts, alors $\exists! A_3 \in S$ tel que $\{A_1, A_2, A_3\} \in \mathcal{D}$.

(III) $|\mathcal{D} > 2|$.

Construisons un $\mathcal{S}_3$-système à partir d'un ev :
Soit E un $\mathbb{F}_2$-espace vectoriel de dimension 3, et prenons $S = E \backslash \{0_E\}$. Pour chaque plan P de E, on associe $D_P = P \backslash \{0_E\}$, et on note $\mathcal{D}$ l'ensemble $\{D_P | P \text{ un plan de E}\}$. Nous allons vérifier que $(S, \mathcal{D})$ est un $\mathcal{S}_3$-système :

- $|E| = 8 \Rightarrow |S| = 7$ donc S est non-vide.
- Soit P un plan de E, il est engendré par deux vecteurs non-nuls et non colinéaires de E, notons-les u et v. Alors $P = \{\lambda u + \mu v | \lambda, \mu \in \mathbb{F}_2\}$, et contient exactement 4 éléments : 0, u, v, et $u + v$. Ainsi D_P contient 3 éléments, et $\mathcal{D}$ est bien un ensemble de 3-parties de S.

— Soient P et P' deux plans distincts de E, alors leur intersection est une droite d de E. d est engendré par un vecteur x, et peut donc s'écrire $d = \{\lambda x \mid \lambda \in \mathbb{F}_2\} = \{0, x\}$. Ainsi, $D_P \cap D_{P'} = P \cap P' \backslash \{0_E\} = d \backslash \{0_E\} = \{x\}$, et la propriété (I) est vérifiée.
— Soient x et y deux vecteurs distincts non-nuls de E. x et y ne sont jamais colinéaires, en effet, $\exists \lambda \in \mathbb{F}_2^*$ tel que $x = \lambda y \Leftrightarrow x = y$. Donc, x et y engendrent un unique plan P_{xy}, contenant $x+y$, et $D_{P_{xy}} = \{x, y, x+y\} \in \mathcal{D}$. On a vérifié la propriété (II).
— Enfin, il y a autant d'éléments dans $\mathcal{D}$ que de plans dans E. Chaque plan à un unique vecteur normal défini selon le produit scalaire usuel, ainsi, il y a autant de plans dans E que de vecteurs non-nuls dans E, c'est-à-dire 7. On a ainsi vérifié la propriété (III).

Nous avons construit un $\mathcal{S}_3$-système à partir d'un $\mathbb{F}_2$-espace vectoriel E, on l'appelera $\mathcal{S}_3$-système issu de E. Nous allons montrer que tous les $\mathcal{S}_3$-système sont de cette forme :

Théorème 3.1. *Soit $(S, \mathcal{D})$ un $\mathcal{S}_3$-système, et soit $\underline{O} \notin S$, alors il existe une unique structure de $\mathbb{F}_2$-espace vectoriel sur $E = S \cup \{\underline{O}\}$ telle que $\dim_{\mathbb{F}_2}(E) = 3$, $0_E = \underline{O}$, et $(S, \mathcal{D})$ est le $\mathcal{S}_3$-système issu de E.*

Notamment, $|S| = 7 = |\mathcal{D}|$.

Démonstration. On définit une loi d'addition interne sur E :
— $\forall x \in E$, $\underline{O} + x = x + \underline{O} = x$, c'est-à-dire que $\underline{O}$ est l'élément neutre de cette loi ;
— $\forall x \in E$, $x + x = \underline{O}$, donc x est son propre inverse ;
— $\forall x, y \in E \backslash \{\underline{O}\}$, on sait par la propriété (II) qu'il existe un unique $z \in S$ tel que $\{x, y, z\} \in \mathcal{D}$. On définit alors $x + y = z$. Cette définition rend la loi commutative.

Il faut vérifier l'associativité de cette loi : soient $x, y, z \in E$, alors, si deux d'entre eux sont égaux, ou si l'un d'entre eux est $\underline{O}$, ou encore si $\{x, y, z\} \in \mathcal{D}$alors l'associativité est évidente. Dans le cas contraire, on a $x+y = z_1 \neq z$, et $z_1+z = z_2$, c'est-à-dire $(x+y)+z = z_2$, et $y+z = x_1$. Notre but est de montrer $x+x_1 = z_2$, c'est-à-dire $\{x, x_1, z_2\} \in \mathcal{D}$.

On a $\{z, z_1, z_2\} \in \mathcal{D}$ et $\{y, z, x_1\} \in \mathcal{D}$, donc $\{z, z_1, z_2\} \cap \{y, z, x_1\} = \{z\}$ car $z_1 \neq z$, $z_1 = x + y \neq y$ car $x \neq \underline{O}$, et $z_1 = x + y \neq z + y = x_1$, car $z \neq x$. Ainsi, $z_1 \notin \{z, y, x_1\}$, donc d'après la propriété (I), l'intersection est réduite à un singleton.

De même $\{y, z, x_1\} \cap \{x, y, z_1\} = \{y\}$. On a notamment $x_1 \neq x$ et $x_1 \neq z_2$. Notons D l'unique élément de $\mathcal{D}$ contenant x et x_1. D rencontre $D' = \{z, z_1, z_2\}$ en un seul point, car $x_1 \notin D'$. Ce ne peut être ni z ni z_1, car $\{x, x_1, z\} \cap \{y, z, x_1\} \subset \{x_1, z\}$, et $x \neq y$; de même $\{x, x_1, z_1\} \cap \{x, y, z_1\} \subset \{x, z_1\}$ et $y \neq x_1 = y + z$. Ainsi, $\{x, x_1, z_2\} \in \mathcal{D}$.

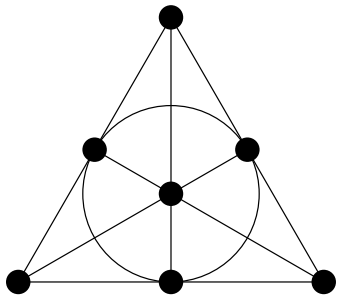
$(E, +)$ est donc un groupe abélien, de neutre $\underline{O}$, avec $\forall x \in E$, $x + x = \underline{O}$. On défini une loi externe $\cdot$ sur $\mathbb{F}_2 \times E$ par $0 \cdot x = \underline{O}$ et $1 \cdot x = x$, ainsi E est un

$\mathbb{F}_2$-espace vectoriel avec $\underline{O} = 0_E$.

Par la définition de l'addition dans E, si $D = \{x, y, z\} \in \mathcal{D}$, alors $z = x + y$, et $D \cup \{\underline{O}\} = \{\underline{O}, x, y, x + y\}$ est le plan engendré par x et y dans E. Comme $|D| > 2$ d'après (III), on a au moins deux plans distincts dans E, ce qui signifie que $\dim_{\mathbb{F}_2}(E) > 2$. D'après la propriété (I), il n'y a pas de plan de E qui ne se croise qu'en $\underline{O}$, ce qui implique que $\dim_{\mathbb{F}_2}(E) < 3$. On a alors prouvé que $(S, \mathcal{D})$ est issu de E, et en particulier, $|S| = 7 = |\mathcal{D}|$.

Il nous reste à prouver l'unicité de cette structure. En effet, si $(S, \mathcal{D})$ est issu de E, alors les plans de E sont de la forme $\{\underline{O}, x, y, x + y\}$, et donc les $D \in \mathcal{D}$ sont de la forme $\{x, y, x + y\}$, c'est-à-dire que la loi d'addition est celle définie précédément. □

Un $\mathcal{S}_3$-système est souvent représenté sous cette



Les 7 points représentent les éléments de S, et les 7 lignes représentent les éléments de $\mathcal{D}$.

Soient $(S, \mathcal{D})$ et $(S', \mathcal{D}')$ deux $\mathcal{S}_3$-système, et θ une bijection de S dans S'. On dit que θ est un isomorphisme s'il induit une bijection de $\mathcal{D}$ dans $\mathcal{D}'$. Deux $\mathcal{S}_3$-système sont isomorphes quand il existe un isomorphisme entre eux. Or, tous les $\mathbb{F}_2$-espace vectoriel de dimension 3 sont isomorphes, et les isomorphismes entre $\mathbb{F}_2$-espaces vectoriels envoient chaque plan sur un plan. Ainsi, deux $\mathcal{S}_3$-système issus de $\mathbb{F}_2$-espaces vectoriels sont isomorphes, et d'après le théorème 3.1, tous les $\mathcal{S}_3$-système sont isomorphes.

Enfin, les automorphismes d'un $\mathcal{S}_3$-système $(S, \mathcal{D})$ forment un sous-groupe du groupe des permutations de S. Comme les automorphismes de $(S, \mathcal{D})$ correspondent aux automorphismes de E, l'espace vectoriel duquel $(s, \mathcal{D})$ est issu, le groupe des automorphismes de $(S, \mathcal{D})$ est isomorphe à $\mathrm{GL}_{\mathbb{F}_2}(E)$, lui-même isomorphe à $PSL_{\mathbb{F}_2}(E) = PSL(3, \mathbb{F}_2)$ d'après les résultats précédents. On retiendra donc :

Théorème 3.2. *Les automorphismes d'un $\mathcal{S}_3$-système forment un groupe isomorphe à $PSL(3, \mathbb{F}_2)$, qui est un groupe simple d'ordre 168.*

3.2 Action sur ce plan

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur un ensemble S à 7 éléments. Soit Φ associé à cette action : $\begin{smallmatrix} G \to & \mathfrak{S}_S \\ g \to \Phi(g): & S \to S \\ & x \to gx \end{smallmatrix}$

$\ker(\Phi) \neq G$, car l'action est transitive. Comme G est simple, $\ker(\Phi) = \{e_G\}$, ce qui signifie que Φ est injective. G s'identifie donc à une sous-groupe de $\mathfrak{S}_S = \mathfrak{S}_7$ par l'intermédiaire de Φ. On a dans un premier temps :

- $G \in A_7$, en effet, si l'on note s la signature, on a $G/\ker(s) = s(G)$, ce qui signifie $[G : \ker(s)] = |s(G)|$. Si $s(G) = 2$, auquel cas $\ker(s)$ est d'indice 2, donc distingué dans G, ce qui est impossible car G est simple. Donc, $s(G) = 1$, ce qui signifie $G \subset A_7$.
- G contient un élément d'ordre 7, car $7|168$. Or un élément d'ordre 7 dans $\mathfrak{S}_7$ est un 7-cycle.
- A_7 est engendré par tout couple $\{u, v\}$ où u est un 7-cycle et v un 3-cycle [2]. Ainsi, G ne peut contenir aucun 3-cycle, sinon il serait égal à A_7 et donc de cardinal 2520.
- G contient un élément d'ordre 2 car $2|168$. Or, les seuls élément de A_7 d'ordre 2 sont des bitranspostions, c'est-à-dire des produits de transpositions disjointes. Chacun de ces éléments a 3 points fixes dans 7.

Théorème 3.3. *Soit $\mathcal{D}$ l'ensemble des 3-parties de S fixées par une bitransposition de G. Alors, $(S, \mathcal{D})$ est un $\mathcal{S}_3$-système.*

Démonstration. Soient a et b deux éléments distincts de S, notons $G_a = \{g \in G \mid ga = a\}$ et G_b les stabilisateurs de a et b. Ils sont conjugués dans G, et ont pour cardinal $\frac{|G|}{|O_a|} = 24$ car $O_a = S$. Soit $\mathcal{E} = S \backslash \{a, b\}$ et $H = G_a \cap G_b$. Par restriction de l'action de G sur S, on obtient une action fidèle de H sur $\mathcal{E}$, donc H s'identifie à un sous-groupe de $\mathfrak{S}_\mathcal{E}$. Cette action n'est pas transitive : si elle l'était, on aurait $|\mathcal{E}|\big||H| \Rightarrow 5\big||G| = 168$. Supposons maintenant que cette action n'admet aucun point fixe, alors, ses orbites sont au nombre de 2, ω_2 de cardinal 2 et ω_3 de cardinal 3. Cela signifie qu'il existe un 3-cycle de support ω_3 dans H, donc dans G, mais G ne contient pas de 3-cycle.

Ainsi H fixe au moins un point sur $\mathcal{E}$, notons-le c. Ainsi, H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, et comme il ne contient pas de 3-cycle, il est composé de l'identité et de bitranspositions laissant fixe $\{a, b, c\}$. H n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments. Donc H contient au moins une bitranspostion, c'est-à-dire pour a et b distincts dans S, il existe une bitransposition de G laissant invariant a, b, et un autre point c de S ; de plus, toutes les bistransposition de G laissant fixe a et b laissent seulement a, b, et$c$ fixes : on a vérifié la propriété (II).

2. La preuve se trouve en annexe.

De plus, $|S| = 7$: prenons a, $b \in S$, alors $\exists c \in S$ tel que $\{a, b, c\} \in \mathcal{D}$. Prenons alors a', $b' \in S\backslash\{a, b, c\}$, alors $\exists c' \in S$ tel que $\{a', b', c'\} \in \mathcal{D}$. Donc $|\mathcal{D}| > 2$, et on a vérifié la propriété (III).

Enfin, montrons que deux éléments distincts de $\mathcal{D}$ se croisent en un seul point de S. On sait qu'ils se croisent en au plus un point, car s'ils se croisent en deux points, alors la propriété (II) garantit qu'ils se croisent en trois points, c'est-à-dire qu'ils sont égaux. Supposons alors qu'il existe u et v des bitranspositions de G dont les ensembles de point fixes D_u et D_v sont disjoints. Soit $\{c\} = S\backslash(D_u \cup D_v)$. Étudions l'orbite de c par $\sigma = (uv)^2$:

— $v(c) \in Supp(v)$, $v(c) \neq c$, et $Supp(u) \cap Supp(v) = c$, donc $u(v(c)) = v(c)$; ainsi $\sigma(c) = u(v(u(v(c)))) = u(v(v(c))) = u(c)$ car v est d'ordre 2.
— Un argument similaire permet d'obtenir $\sigma(u(c)) = v(c)$, et $\sigma(v(c)) = c$.
— Soit $x \in Supp(v)\backslash\{c, v(c)\}$. Alors $v(x) \in Supp(v)\backslash\{c, v(c)\}$, donc $v(x) \notin Supp(u)$, c'est-à-dire $u(v(x)) = v(x)$, d'où $\sigma(x) = x$.
— Similairement, si $x \in Supp(u)\backslash\{c, u(c)\}$, $\sigma(x) = x$.

On obtient donc $\sigma = (c, u(c), v(c))$ est un 3-cycle dans G. Or G ne contient pas de 3-cycle, donc deux bitranspositions se croisent toujours en un seul point, et on a vérifié la propriété (I). □

On peut alors démontrer le théorème suivant :

Théorème 3.4. *Soit G un groupe simple d'ordre 168 agissant transitivement sur un ensemble S à 7 éléments. Alors, G est isomorphe à $PSL(3, \mathbb{F}_2)$.*

Démonstration. Notre but est de montrer que les éléments de G sont des automorphismes du $\mathcal{S}_3$-système obtenu par l'action de G sur S. Soit donc $\mathcal{D}$ l'ensemble des 3-parties laissées fixes par les bitranspositions de G, et soient $g \in G$ et $D \in \mathcal{D}$. Choisissons u une involution de G dont l'ensemble des points fixes est D, alors $v = gug^{-1}$ est une involution dont $g(D)$ est l'ensemble des points fixes, c'est-à-dire $g(D) \in \mathcal{D}$, ce qui signifie que g est un automorphisme de $(S, \mathcal{D})$.

Ainsi, $G \subset Aut(S, \mathcal{D})$, mais on sait d'après le théorème 3.2 que le groupe des automorphismes d'un $\mathcal{S}_3$-système est isomorphe à $PSL(3, \mathbb{F}_2)$, donc en particulier, son cardinal est 168. Ce qui signifie $G = Aut(S, \mathcal{D}) = PSL(3, \mathbb{F}_2)$. □

3.3 Unicité du groupe simple d'ordre 168

Soit G un groupe simple de cardinal $168 = 2^3 \cdot 3 \cdot 7$. Nous allons déterminer précisément quels sont les p-Syllow de G, puis nous servir des propriétés des sous-groupes de G pour construire une action de G sur un ensemble à 7 éléments.

Pour i premier divisant 168, on notera $\mathcal{S}_i$ l'ensemble des i-Sylow de G ; on a $\mathcal{S}_i > 1$ par simplicité ce G. Pour k divisant 168, on notera $\mathcal{O}_k$ l'ensemble des éléments de G d'ordre k, et $\mathcal{G}_k$ l'ensemble des sous-groupes de G de cardinal k. Pour $u \in G$, on note $\mathcal{Z}_u = \{v \in G \mid uv = vu\}$ le centralisateur de u dans G.

Outre les théorèmes de Sylow, on utilisera dans la suite une propriété découlant immédiatement des théorèmes de Sylow : Soit p un nombre premier, $m \in \{1, \dots, p-1\}$, et G un groupe de cardinal $n = pm$. On sait que le nombre de p-Sylow de G est congru à 1 modulo p, et qu'il divise $m < p$; donc il y a un seul p-Syllow dans G.

3.3.1 Étude des 7-Sylow

On a par un théorème de Sylow $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7||24$. Les seules possibilités sont 1 et 8 ; mais on sait qu'il n'y en a pas qu'un seul, sinon, il serait distingué, donc $|\mathcal{S}_7| = 8$. Soit H et H' deux 7-Sylow distincts, alors $H \cap H' = \{1_G\}$; en effet, les éléments de H et H' sont tous d'ordre 7, donc $|H \cap H'| > 1 \Rightarrow |H \cap H'| = 7$, donc $H = H'$. On obtient alors le nombre total d'éléments d'ordre 7 dans G : $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$. L'action de G sur $\mathcal{S}_7$ par conjugaison est transitive et fidèle, et permet d'identifier G à un sous-groupe de $\mathfrak{S}_{\mathcal{S}_7} \cong \mathfrak{S}_8$. Soit s la signature sur G vu comme sous-groupe de $\mathfrak{S}_8$, alors $\ker(s)$ est d'indice $|\operatorname{Im}(s)|$ dans G ; il ne peut pas être d'indice 2 car G est simple, donc $|\operatorname{Im}(s)| = 1$ et $G \subset \mathfrak{A}_8$.

Pour $H \in \mathcal{S}_7$, le stabilisateur de H dans G est aussi le normalisateur de H dans G, on le note $\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$. On a $\frac{|\mathcal{N}_G(H)|}{|G|} = |\mathcal{S}_7|$, donc $|\mathcal{N}_G(H)| = 21$; or G ne peut pas contenir d'éléments d'ordre 21, car un tel élément devrait contenir dans sa décomposotion en cycles disjoints au moins un 7-cycle et un 3-cycle, ce qui est impossible dans $\mathfrak{S}_8$. Enfin, $\mathcal{N}_G(H)$ ne contient qu'un seul sous-groupe de cardinal 7, car son cardinal est $21 = 3 \cdot 7$. De plus, nous avons démontré que les seuls éléments qui permutent avec des éléments d'ordre 7 sont d'ordre 3 ou 7.

Ainsi $\mathcal{N}_G(H)$ est composé de l'éléments neutre, de 6 éléments d'ordre 7, et 14 éléments d'ordre 3. Soit H et H' deux éléments distincts de $\mathcal{S}_7$. Le groupe $I = \mathcal{N}_G(H) \cap \mathcal{N}_G(H')$ s'identifie à un groupe de permutations de $\mathcal{S}_7 \backslash \{H, H'\}$, qui contient 6 éléments ; donc I ne contient aucun élément d'ordre 7. On sait de plus que $I \neq \{1_G\}$, car sinon G contiendrait au moins $21^2 = 441$ éléments. Ainsi I est un 3-sous-groupe de G, autrement dit un 3-Sylow, et contient 2 éléments d'ordre 3. Ceci implique que $\mathcal{N}_G(H) \cup \mathcal{N}_G(H')$ contient 26 éléments d'ordre 3, et donc $|\mathcal{O}_3| \geqslant 26$. L'étude de I montre aussi que les $\mathcal{N}_G(H)$, où H parcourt $\mathcal{S}_7$, sont tous distincts. On a vu par ailleurs qu'un sous-groupe d'ordre 21 contient un seul 7-Sylow, qui est donc simple dans ce sous-groupe, ce qui signifie que tout sous-groupe de G d'ordre 21 est un stabilisateur d'un 7-Sylow de G.

3.3.2 Étude des 3-Sylow

On procède de la même manière que précédemment pour déterminer que le nombre de 3-Sylow est soit 4, soit 7, soit 28. L'intersection de deux 3-Sylow distincts est $\{1_G\}$, et tout élément d'ordre 3 engendre un 3-Sylow ; donc

$|\mathcal{O}_3| = 2|\mathcal{S}_3|$. Comme $|\mathcal{O}_3| \geqslant 26$, on a nécessairement $|\mathcal{S}_3| = 28$ et $|\mathcal{O}_3| = 56$.

L'action de G par conjugaison sur $\mathcal{S}_3$ est fidèle et transitive, donc pour $H \in \mathcal{S}_3$, le normalisateur $\mathcal{N}_G(H)$ est de cardinal $\frac{|G|}{|\mathcal{S}_3|} = 6$. Tous ces normalisateurs étant conjugués dans G, ils sont soit tous isomorphes à $\mathfrak{S}_3$, soit tous isomorphes à $\mathbb{Z}/6\mathbb{Z}$. De plus, un sous-groupe de cardinal 6 a exactement un sous-groupe d'ordre 3, donc pour H et H' deux 3-Sylow distincts, $\mathcal{N}_G(H) \neq \mathcal{N}_G(H')$.

Supposons qu'il existe dans G un élément x d'ordre 6, alors x engendre un sous-groupe de cardinal 6, et x^2 un sous-groupe de cardinal 3 qui est donc un 3-Sylow. Par conséquent, $< x >= \mathcal{N}_G(< x^2 >)$, et donc tous les $\mathcal{N}_G(H)$, où H parcourt $\mathcal{S}_3$, sont isomorphes à $\mathbb{Z}/6\mathbb{Z}$. Alors tous les 3-Sylow sont engendrés par des carrés d'éléments d'ordre 6, donc l'application $\mathcal{O}_6 \to \mathcal{O}_3$, $u \to u^2$ est surjective. Alors $\mathcal{O}_6 \geqslant 56$: G contient 1 élément d'ordre 1, 48 éléments d'ordre 7, 56 éléments d'ordre 3 et au moins 56 elements d'ordre 6. Donc G contient au plus 7 éléments d'ordre 2, c'est-à-dire un seul 2-Sylow de cardinal 8, ce qui contredit la simplicité de G.

Ainsi $|\mathcal{O}_6| = 0$, et les $\mathcal{N}_G(H)$, où H parcourt $\mathcal{S}_3$, sont tous isomorphes à $\mathfrak{S}_3$. Cette étude prouve de plus que ce sont les seuls sous-groupes de G de cardinal 6, et aucun élément d'ordre 2 ne permute avec un élément d'ordre 3, sinon on obtiendrait un élément d'ordre 6.

3.3.3 Étude des 2-Sylow

On a vu précédemment que les éléments de G d'ordre impair sont soit d'ordre 1, soit d'ordre 3 ou soit d'ordre 7. Définissons R l'ensemble des éléments de G d'ordre pair ; alors $|R| = |G| - |\mathcal{O}_3| - |\mathcal{O}_7| - 1 = 63$. A priori, les éléments de R peuvent être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84. On a cependant prouvé qu'il n'y a pas d'élément d'ordre 6, s'ensuit qu'il n'y pas non plus d'élément d'ordre 12, 24, 42 ou 84. Un élément d'ordre 8 dans G vu comme un sous-groupe de $\mathfrak{S}_8$ est nécessairement un 8-cycle, qui est une permutation impaire, ce qui contredit l'inclusion de G dans $\mathfrak{A}_8$. Il n'y a donc pas d'élément d'ordre 8, ni a fortiori d'élément d'ordre 56, dans G. Enfin, la décomposition en cycles disjoints d'un élément d'ordre 14 contient au moins un 7-cycle et un 2-cycle, ce qui est impossible dans $\mathfrak{S}_8$. Il n'y a donc aucun élément d'ordre 14 ou 28 dans G. Ainsi $R = \mathcal{O}_2 \cup \mathcal{O}_4$, et $R \cup \{1_G\} = \bigcup_{H \in \mathcal{S}_2} H$.

Les diviseurs impairs de 168 sont 1, 3, 7 et 21. Par ailleurs, $R = \bigcup_{H \in \mathcal{S}_2} (H \backslash \{1_G\})$, donc $63 \leqslant 7 \cdot |\mathcal{S}_2|$, ce qui donne $|\mathcal{S}_2| \geqslant 9$, donc il y a 21 2-Sylow dans G. De plus, on sait qu'il existe H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, car sinon, on aurait $21 \cdot 7$ éléments d'ordre pair dans G, ce qui contredit $|R| = 63$.

Soit $u \in \mathcal{O}_2$. On a vu que $\mathcal{Z}_u$ ne contient aucun élément d'ordre 3 ou 7, donc aucun élément de G d'ordre impair, on en déduit que son cardinal est 2, 4, ou 8. Supposons qu'il existe un 2-Sylow abélien, alors tous les 2-Sylow sont abéliens.

Soient H et H' des 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, alors il existe v d'ordre 2 dans $H \cap H'$. Alors $H \cup H' \subset \mathcal{Z}_v$, mais $|H \cup H'| > 8$, ce qui est absurde ; donc les 2-Sylow ne sont pas abéliens, ils sont soit quaternioniques, soit diédraux de degré 4 [3] ; dans les deux cas, $|\mathcal{O}_4| \neq 0$.

Soit $f : \mathcal{O}_4 \to \mathcal{O}_2$, $u \to u^2$; posons $\mathcal{O}'_2 = f(\mathcal{O}_4)$. Pour $v \in \mathcal{O}'_2$, $|f^{-1}(v)| \geqslant 2$. Fixons $v_0 \in \mathcal{O}'_2$, et notons $\mathcal{O}''_2$ sa classe de conjugaison dans G. On a $|\mathcal{O}''_2| = \frac{|G|}{|\mathcal{Z}_{v_0}|}$, qui vaut 21, 42, ou 84. Ainsi $|\mathcal{O}_2| \geqslant |\mathcal{O}''_2| \geqslant 21$, et $|\mathcal{O}_4| \geqslant 2 \cdot |\mathcal{O}'_2| \geqslant 42$. Comme $|\mathcal{O}_4| + |\mathcal{O}_2| = 63$, on en déduit $|\mathcal{O}_4| = 42$ et $|\mathcal{O}_2| = 21$. De plus, $\mathcal{O}_2$ est la classe de conjugaison de n'importe quel élément d'ordre 2, ce qui signifie aussi que tous les éléments d'ordre 2 sont conjugués dans G. Enfin, on obtient pour u d'ordre 2 dans G que $|\mathcal{Z}_u| = 8$, c'est donc un 2-Sylow.

Si les 2-Sylow étaient quaternioniques, alors pour u d'ordre 2, $f^{-1}(u)$ contiendrait au moins les 6 éléments d'ordre 4 de $\mathcal{Z}_u$, ce qui donnerait $|\mathcal{O}_4| \geqslant 6 \cdot |\mathcal{O}_2| = 126$, or $|\mathcal{O}_4| = 42$. Ainsi les 2-Sylow sont tous diédraux de degré 4.

Notons enfin que $[G : \mathcal{N}_G(H)] = |\mathcal{S}_2| = 21$, ce qui donne $|\mathcal{N}_G(H)| = 8 = |H|$, donc $\mathcal{N}_G(H) = H$.

3.4 Sous-groupes de Klein de G

Notons $\mathcal{K}$ l'ensemble de sous-groupes de Klein de G, c'est-à-dire les sous-groupes de G non cycliques de cardinal 4. Soit $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$, alors $H \subset \mathcal{Z}_u$, qui est un 2-Sylow. Comme les 2-Sylow sont diédraux de degré 4, leur centre est un groupe cyclique de cardinal 2, autrement dit, $C(\mathcal{Z}_u) = \{1_G, u\}$, donc pour u et v distincts dans $H \backslash \{1_G\}$, $\mathcal{Z}_u \neq \mathcal{Z}_v$, et H est inclus dans au moins 3 2-Sylow dinstincts.
Soit Γ un 2-Sylow, alors il contient 2 sous-groupes de Klein distincts, dont l'intersection est le centre de Γ.
Enfin, soient $H \in \mathcal{K}$ et $\Gamma \in \mathcal{S}_2$ avec $H \subset \Gamma$; alors $u \in C(\Gamma) \backslash \{1_G\}$ est aussi élément de H, et donc $\Gamma = \mathcal{Z}_u$. Ainsi chaque $H \in \mathcal{K}$ est contenu dans exactement 3 2-Sylow, et chaque 2-Sylow contient exactement 2 sous-groupes de Klein. Ainsi, en dénombrant les couples $(H, \Gamma) \in \mathcal{K} \times \mathcal{S}_2$ tels que $H \subset \Gamma$, on obtient :

$$3 \cdot |\mathcal{K}| = 2 \cdot |\mathcal{S}_2| = 42, \text{ donc } |\mathcal{K}| = 14.$$

Étudions finalement $\mathcal{N}_G(H)$ pour $H \in \mathcal{K}$: il contient $\mathcal{Z}_u$ pour $u \in H \backslash \{1_G\}$, donc possède au moins 16 éléments distincts.
Un élément $u \in H \backslash \{1_G\}$ a $\frac{|G|}{|\mathcal{Z}_u|} = 21$ conjugués dans G. Ainsi, il y a au moins 7 conjugués de H distincts, donc $|\mathcal{N}_G(H)| \leqslant \frac{|G|}{7} = 24$. Comme $|H| = 4$, $|\mathcal{N}_G(H)|$ est un multiple de 4 qui divise 164, compris entre 16 et 24 ; la seule possibilité est $|\mathcal{N}_G(H)| = 24$, et H possède 7 conjugués. Ainsi $\mathcal{K}$ est l'union de deux classes de conjugaison, chacun formée de 7 sous-groupes de G. Nous pouvons désormais démontrer le théorème suivant :

3. Voir en annexe pour une étude précise des groupes d'ordre 8.

Théorème 3.5. *Soit G un groupe simple d'ordre 168, alors G est isomorphe à* $\mathrm{PSL}(3, \mathbb{F}_2)$.

Démonstration. On vient de voir que l'ensemble des sous-groupes de Klein de G posséde deux classes de conjugaison, chacun de cardinal 7. Alors l'action de G sur l'une de ces deux classes est transitive, et d'après le théorème 3.4, G est isomorphe à $\mathrm{PSL}(3, \mathbb{F}_2)$. □

Corollaire 3.1. *Les groupes* $\mathrm{PSL}(2, \mathbb{F}_7)$, $\mathrm{PGL}(2, \mathbb{F}_7)$ *et* $\mathrm{PSL}(3, \mathbb{F}_2)$ *sont tous isomorphes.*

Conclusion

L'isomorphisme que nous venons de trouver entre $\mathrm{PSL}(2, \mathbb{F}_7)$ et $\mathrm{PSL}(3, \mathbb{F}_2)$ provient d'un théorème beaucoup plus puissant, car on a en vérité montré que tous les groupes simples d'ordre 168 sont isomorphes. L'étude réalisée ici montre à quel point classifier les groupes simples peut être une tâche fastidieuse, mêlant souvent des résultats pointus de théorie des groupes, de géométrie, et de théorie des espaces vectoriels. Malgré les travaux de très nombreux mathématiciens sur le sujet, de nombreuses conjectures restent encore insolubles, concernant par exemple le groupe monstre, le plus grand des groupes sporadiques.

Références

[1] Richard ; Solomon Ronald Gorenstein, Daniel ; Lyons. *The classification of the finite simple groups.* American Mathematical Society, 1994-2005.

Annexes

$\mathfrak{A}_7$ est engendré par tout couple d'un 3-cycle et d'un 7-cycle

Soient u un 3-cycle et v un 7-cycle, tous deux dans $\mathfrak{A}_7$. Pour des raisons pratiques et sans perte de généralité, on supposera que l'ensemble à 7 éléments sur lequel on effectue les permutations est $\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$. Si l'on note $u = (a\ b\ c)$ avec $a, b, c \in \mathbb{F}_7$, alors il existe $k \in \mathbb{Z}$ tel que $v^k(a) = b$. On peut alors réordonner $\mathbb{F}_7$, et prendre $u = (1\ 2\ x)$, avec $x \in \mathbb{F}_7$, et $v = (1\ 2\ 3\ 4\ 5\ 6\ 7)$.

(1) En conjuguant u par v, on obtient $vuv^{-1} = (2\ 3\ x+1)$, avec la règle d'addition de $\mathbb{F}_7$. Montrons que quelle que soit la valeur de x, on peut à partir de u et v obtenir le cycle $(1\ 2\ 3)$.

   (a) Si $x = 3$, alors il n'y a rien à prouver.

   (b) Si $x = 4$, alors on définit $w = v^2uv^{-2} = (3\ 4\ 6)$. On a $w^2uw^{-2} = (1\ 2\ 3)$.

   (c) Si $x = 5$, alors on définit $w = v^3uv^{-3} = (4\ 5\ 1)$. On a $wuw^{-1} = (4\ 2\ 1) = (1\ 2\ 4)^{-1}$. On procède ensuite comme dans le cas $x = 4$ pour obtenir $(1\ 2\ 3)$.

   (d) Si $x = 6$, alors on définit $w = v^3uv^{-3} = (5\ 6\ 3)$. On a $wuw^{-1} = (1\ 2\ 3)$.

   (e) Si $x = 7$, alors $vuv^{-1} = (2\ 3\ 1) = (1\ 2\ 3)^{-1}$.

   Ainsi $(1\ 2\ 3)$ peut toujours être obtenu à partir de u et v.

(2) À partir de $(1\ 2\ 3)$ et v, on peut obtenir tout 3-cycle de la forme $(1\ 2\ y)$, avec $y \in \mathbb{F}_7$. En effet, posons $w = v^2(1\ 2\ 3)v^{-2} = (3\ 4\ 5)$; alors $w(1\ 2\ 3)w^{-1} = (1\ 2\ 4)$ et $w(1\ 2\ 4)w^{-1} = (1\ 2\ 5)$. Posons ensuite $w' = v^4(1\ 2\ 3)v^{-4} = (5\ 6\ 7)$; alors $w'(1\ 2\ 5)w'^{-1} = (1\ 2\ 6)$ et $w'(1\ 2\ 6)w'^{-1} = (1\ 2\ 7)$.

(3) Montrons que l'on peut en fait obtenir tous les 3-cycles à partir de u et v. En effet, on peut d'ores et déjà obtenir par conjugaison des 3-cycles de la forme $(1\ 2\ x)$ par v, tous les 3-cycles de la forme $(x\ x+1\ y)$ avec $x, y \in \mathbb{F}_7$, ainsi que leurs inverses $(y\ x+1\ x)$. Soit alors $(a\ b\ c)$ un 3-cycle de $\mathfrak{A}_7$. Si $b = a + 1$, on sait déjà que ce cycle est engendré par u et v. Sinon, on peut écrire $(a\ b\ c) = (a\ a+1\ c)(b\ a+1\ a)$.

(4) Enfin, $\mathfrak{A}_7$ est engendré par les 3-cycles. En effet, tout produit de deux transpositions peut s'écrire sous la forme de produits de 3-cycles : $(a\ b)(a\ b) = \mathrm{id}$, $(a\ b)(b\ c) = (a\ b\ c)$, et $(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$.

Ainsi $\mathfrak{A}_7$ est engendré par n'importe quel couple (u, v) avec u un 3-cycle et v un 7-cycle.

Un groupe d'ordre 8 est abélien, diédral, ou quaternionique

Soit G un groupe d'ordre 8. Les éléments de $G\backslash\{1_G\}$ sont d'ordre 2, 4 ou 8. On procède par disjonction de cas sur l'existence d'élément de chaque ordre :

(1) S'il existe un élément d'ordre 8, alors G est cyclique, isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

(2) S'il n'existe aucun élément d'ordre 8, ni d'ordre 4, alors G est abélien : en effet, soient a, b dans $G\backslash\{1_G\}$, alors $abab = (ab)^2 = 1_G$, donc $ab = ba$. G est alors isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

(3) S'il n'existe pas d'élément d'ordre 8 mais qu'il existe un élément d'ordre 4, noté a, on considère le sous-groupe $H =< a >$ qui est de cardinal 4, donc d'indice 2 dans G, et donc distingué.

   (a) S'il existe b dans $G\backslash H$ d'ordre 2, alors on note $a' = bab^{-1}$. a' est d'ordre 4, et comme H est distingué, $a' \in H$; donc $a' \in \{a, a^{-1}\}$.

      (i) Si $a' = a$, alors a et b commutent, et donc $< a, b >= G$ commute. G est alors isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

      (ii) Si $a' = a^{-1}$, alors $G =< a, b >$ avec a d'ordre 4, b d'ordre 2, et $bab = a^{-1}$, donc G est isomorphe au groupe diédral de degré 4.

   (b) Si tous les éléments de $G\backslash H$ sont d'ordre 4, alors prenons $b \in G\backslash H$. b^2 est d'ordre 2, donc est dans H, et donc $b^2 = a^2$ qui est le seul élément d'ordre 2 dans H et donc dans G. Considérons comme précédemment $a' = bab^{-1} \in \{a, a^{-1}\}$.

      (i) Si $a' = a$, alors $ab = ba$, et $(ab)^2 = a^2b^2 = a^4 = 1_G$; donc (ab) est d'ordre 1 ou 2. S'il est d'ordre 1, alors $b = a^{-1}$, et s'il est d'ordre 2, alors $ab = a^2$, car c'est le seul élément d'ordre 2, et donc $b = a$. On obtient dans les deux cas une contradiction, donc $a' \neq a$.

      (ii) Ainsi $G =< a, b >$ avec a et b d'orde 4, $a^2 = b^2$, $aba^{-1} = b^{-1}$. Dans ce cas G est isomorphe au groupe quaternionique.

Ainsi, il y a 5 possibilités pour G : il est soit isomorphe à $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^3$, auquel cas il est abélien ; soir isomorphe au groupe diédral de degré 4 ou au groupe quaternionique, auquel cas il est non abélien.

Propriétés des groupes non abéliens d'ordre 8

Dans un groupe quaternionique, il y a 6 éléments d'ordre 4 et un élément d'ordre 2. Cela signifie que si u et v sont d'ordre 4, alors $u^2 = v^2$.
Le centre du groupe diédral de degré 4 est composé de deux éléments. Si l'on le note $< a, b >$ avec a d'ordre 4, b d'ordre 2, et $bab = a^{-1}$, alors le centre est $\{1, a^2\}$. Si l'on voit ce groupe comme le groupe de symmétries d'un carré, alors les éléments centraux sont l'identité et la rotation d'un demi-tour.