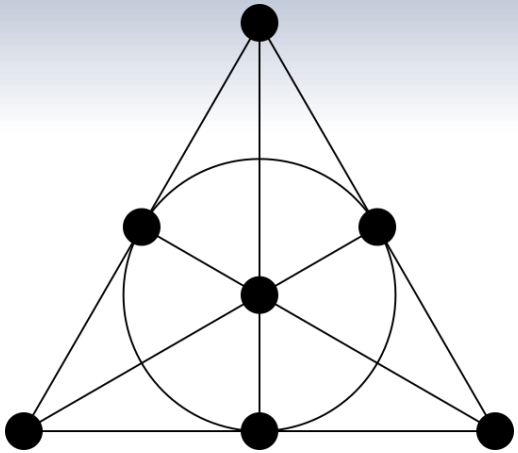
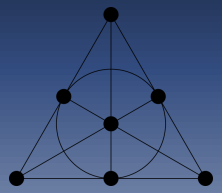


Le groupe simple d'ordre 168

Blaise Boissonneau

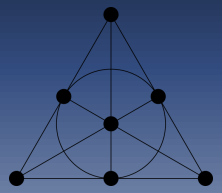
Juin 2017

Université de Lorraine



Introduction

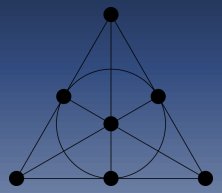
Un groupe simple d'ordre fini est soit :



Introduction

Un groupe simple d'ordre fini est soit :

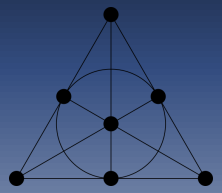
- $\mathbb{Z}/p\mathbb{Z}$, p premier



Introduction

Un groupe simple d'ordre fini est soit :

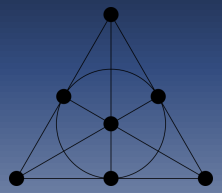
- $\mathbb{Z}/p\mathbb{Z}$, p premier
- $\mathfrak{A}_n$, $n \geqslant 5$



Introduction

Un groupe simple d'ordre fini est soit :

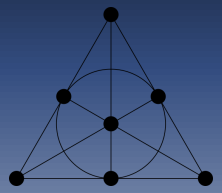
- $\mathbb{Z}/p\mathbb{Z}$, p premier
- $\mathfrak{A}_n$, $n \geqslant 5$
- Membre d'une des 16 familles infinies de groupes de type Lie simples,



Introduction

Un groupe simple d'ordre fini est soit :

- $\mathbb{Z}/p\mathbb{Z}$, p premier
- $\mathfrak{A}_n$, $n \geqslant 5$
- Membre d'une des 16 familles infinies de groupes de type Lie simples,
- Un des 27 groupes sporadiques

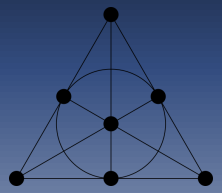


Introduction

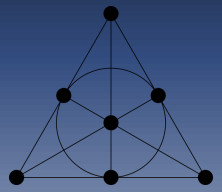
Un groupe simple d'ordre fini est soit :

- $\mathbb{Z}/p\mathbb{Z}$, p premier
- $\mathfrak{A}_n$, $n \geqslant 5$
- Membre d'une des 16 familles infinies de groupes de type Lie simples,
- Un des 27 groupes sporadiques

Nous étudions ici l'une des familles de groupes de type Lie simples, les groupes projectifs spéciaux linéaires, et en détails précis deux d'entre eux, dont on montrera qu'ils sont isomorphes.

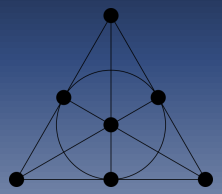


Sommaire



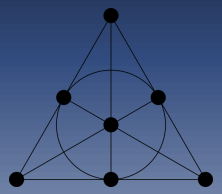
Définitions des groupes étudiés

- $\mathrm{GL}(n, K) : \det^{-1}(K^*)$



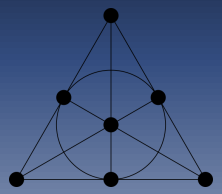
Définitions des groupes étudiés

- $\mathrm{GL}(n, K) : \det^{-1}(K^*)$
- $\mathrm{SL}(n, K) : \det^{-1}(1_K)$



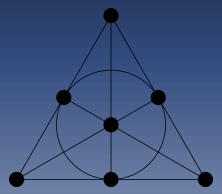
Définitions des groupes étudiés

- $\mathrm{GL}(n, K) : \det^{-1}(K^*)$
- $\mathrm{SL}(n, K) : \det^{-1}(1_K)$
- $\mathcal{H}^*(n, K) : \{\lambda I_n \mid \lambda \in K^*\}$



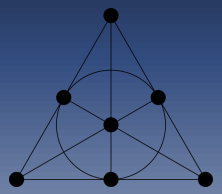
Définitions des groupes étudiés

- $\mathrm{GL}(n, K)$: $\det^{-1}(K^*)$
- $\mathrm{SL}(n, K)$: $\det^{-1}(1_K)$
- $\mathcal{H}^*(n, K)$: $\{\lambda I_n \mid \lambda \in K^*\}$
- $\mathrm{S}\mathcal{H}^*(n, K)$: $\mathrm{SL}(n, K) \cap \mathcal{H}^*(n, K)$



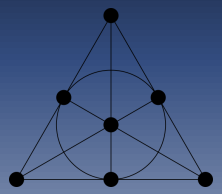
Définitions des groupes étudiés

- $\mathrm{GL}(n, K)$: $\det^{-1}(K^*)$
- $\mathrm{SL}(n, K)$: $\det^{-1}(1_K)$
- $\mathcal{H}^*(n, K)$: $\{\lambda I_n \mid \lambda \in K^*\}$
- $\mathrm{S}\mathcal{H}^*(n, K)$: $\mathrm{SL}(n, K) \cap \mathcal{H}^*(n, K)$
- $\mathrm{PGL}(n, K)$: $\mathrm{GL}(n, K)/\mathcal{H}^*(n, K)$



Définitions des groupes étudiés

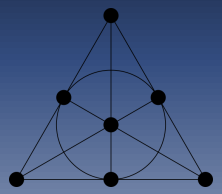
- $\mathrm{GL}(n, K) : \det^{-1}(K^*)$
- $\mathrm{SL}(n, K) : \det^{-1}(1_K)$
- $\mathcal{H}^*(n, K) : \{\lambda I_n \mid \lambda \in K^*\}$
- $\mathrm{S}\mathcal{H}^*(n, K) : \mathrm{SL}(n, K) \cap \mathcal{H}^*(n, K)$
- $\mathrm{PGL}(n, K) : \mathrm{GL}(n, K)/\mathcal{H}^*(n, K)$
- $\mathrm{PSL}(n, K) : \mathrm{SL}(n, K)/\mathrm{S}\mathcal{H}^*(n, K)$



Transvections & dilatations

En notant $E_{i,j}$ les matrices de la base canonique de $\mathfrak{M}_n(K)$ et pour $\lambda \in K$,

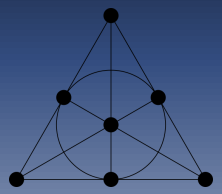
- Une matrice de dilatation notée $D(\lambda)$ est $\mathrm{Diag}(1, \ldots, 1, \lambda)$



Transvections & dilatations

En notant $E_{i,j}$ les matrices de la base canonique de $\mathfrak{M}_n(K)$ et pour $\lambda \in K$,

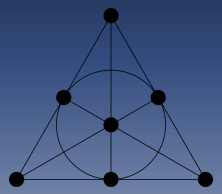
- Une matrice de dilatation notée $D(\lambda)$ est $\mathrm{Diag}(1, \ldots, 1, \lambda)$
- Une matrice de transvection notée $T_{i,j}(\lambda)$ est $I_n + \lambda E_{i,j}$ $(i \neq j)$



Transvections & dilatations

En notant $E_{i,j}$ les matrices de la base canonique de $\mathfrak{M}_n(K)$ et pour $\lambda \in K$,

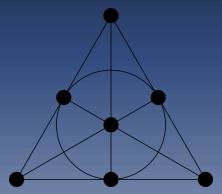
- Une matrice de dilatation notée $D(\lambda)$ est $\mathrm{Diag}(1, \ldots, 1, \lambda)$
- Une matrice de transvection notée $T_{i,j}(\lambda)$ est $I_n + \lambda E_{i,j}$ $(i \neq j)$
- $T_{i,j}(\lambda) \times M$ remplace $\mathcal{L}_i(M)$, la i$^{\text{ème}}$ ligne de M, par $\mathcal{L}_i(M) + \lambda \mathcal{L}_j(M)$



Transvections & dilatations

En notant $E_{i,j}$ les matrices de la base canonique de $\mathfrak{M}_n(K)$ et pour $\lambda \in K$,

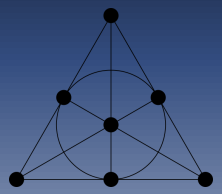
- Une matrice de dilatation notée $D(\lambda)$ est $\mathrm{Diag}(1, \ldots, 1, \lambda)$
- Une matrice de transvection notée $T_{i,j}(\lambda)$ est $I_n + \lambda E_{i,j}$ $(i \neq j)$
- $T_{i,j}(\lambda) \times M$ remplace $\mathcal{L}_i(M)$, la i$^{\text{ème}}$ ligne de M, par $\mathcal{L}_i(M) + \lambda \mathcal{L}_j(M)$
- $M \times T_{i,j}(\lambda)$ remplace $\mathcal{C}_j(M)$ par $\mathcal{C}_j(M) + \lambda \mathcal{C}_i(M)$



Générateurs

Théorème

Pour $M \in \mathrm{GL}(n, K)$, en notant $\lambda = \det(M)$, alors M peut s'écrire $D(\lambda) \times A_1 \times \cdots \times A_r$ ou $B_1 \times \cdots \times B_s \times D(\lambda)$, avec A_k et B_m de transvection.



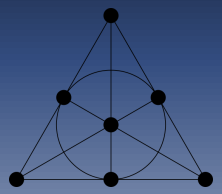
Générateurs

Théorème

Pour $M \in \mathrm{GL}(n, K)$, en notant $\lambda = \det(M)$, alors M peut s'écrire $D(\lambda) \times A_1 \times \cdots \times A_r$ ou $B_1 \times \cdots \times B_s \times D(\lambda)$, avec A_k et B_m de transvection.

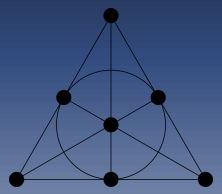
La démonstration se fait par récurrence. Le but est de montrer qu'avec des opérations sur les colonnes, on peut transformer M en une matrice de la forme :

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



Démonstration

On commence par s'assurer que $C_{1,2}(M) \neq 0$. Dans le cas contraire, on ajoute à $\mathcal{C}_2(M)$ une colonne dont la première composante est non nulle ; on sait qu'elle existe car $\det(M) \neq 0$.

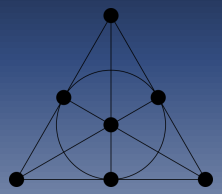


Démonstration

On commence par s'assurer que $C_{1,2}(M) \neq 0$. Dans le cas contraire, on ajoute à $\mathcal{C}_2(M)$ une colonne dont la première composante est non nulle ; on sait qu'elle existe car $\det(M) \neq 0$.

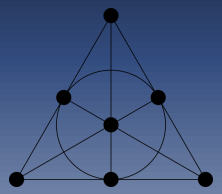
Exemple

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



Démonstration

On remplace ensuite $\mathcal{C}_1(M)$ par $\mathcal{C}_1(M) + \frac{1-C_{1,1}(M_1)}{C_{1,2}(M_1)}\mathcal{C}_2(M)$, ce qui donne $C_{1,1}(M) = 1$.

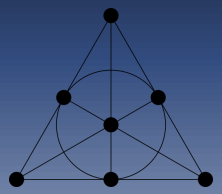


Démonstration

On remplace ensuite $\mathcal{C}_1(M)$ par $\mathcal{C}_1(M) + \frac{1-C_{1,1}(M_1)}{C_{1,2}(M_1)}\mathcal{C}_2(M)$, ce qui donne $C_{1,1}(M) = 1$.

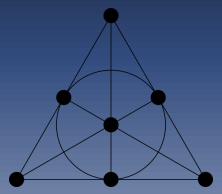
Exemple

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



Démonstration

Ensuite on ajoute $-C_{1,j}(M)\mathcal{C}_1(M)$ à $\mathcal{C}_j(M)$ $(j \neq 1)$, ce qui transforme tous les coefficients de la première ligne en 0 (sauf le premier).

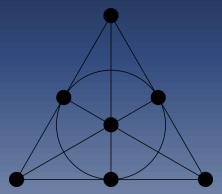


Démonstration

Ensuite on ajoute $-C_{1,j}(M)\mathcal{C}_1(M)$ à $\mathcal{C}_j(M)$ $(j \neq 1)$, ce qui transforme tous les coefficients de la première ligne en 0 (sauf le premier).

Exemple

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



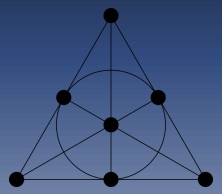
Démonstration

Ensuite on ajoute $-C_{1,j}(M)\mathcal{C}_1(M)$ à $\mathcal{C}_j(M)$ $(j \neq 1)$, ce qui transforme tous les coefficients de la première ligne en 0 (sauf le premier).

Exemple

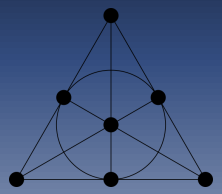
$$\left(\begin{array}{c|c|c} 1 & 2 & -2 \\ 2 & -4 & 9 \\ 2 & 8 & 0 \end{array}\right) \xrightarrow{\times T_{1,2}(-2)} \left(\begin{array}{c|c|c} 1 & 0 & -2 \\ 2 & -8 & 9 \\ 2 & 4 & 0 \end{array}\right)$$

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



Démonstration

Comme $\det(M) = \det(N) \neq 0$, on a $X = N \times \overbrace{N^{-1} \times X}^{\xi}$, donc en soustrayant $\xi_1 \mathcal{C}_2(M) + \cdots + \xi_{n-1} \mathcal{C}_n(M)$ à $\mathcal{C}_1(M)$, on obtient la matrice voulue.

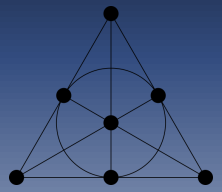


Démonstration

Comme $\det(M) = \det(N) \neq 0$, on a $X = N \times \overbrace{N^{-1} \times X}^{\xi}$, donc en soustrayant $\xi_1 \mathcal{C}_2(M) + \cdots + \xi_{n-1} \mathcal{C}_n(M)$ à $\mathcal{C}_1(M)$, on obtient la matrice voulue.

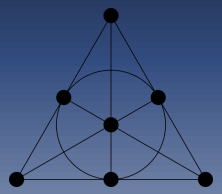
Exemple

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



Démonstration

On applique le même raisonnement à la sous-matrice.

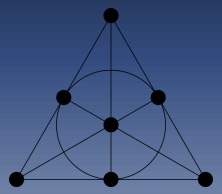


Démonstration

On applique le même raisonnement à la sous-matrice.

Exemple

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



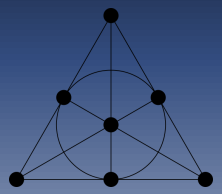
Démonstration

On applique le même raisonnement à la sous-matrice.

Exemple

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

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



Démonstration

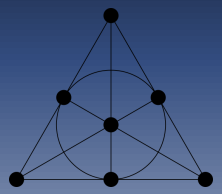
On applique le même raisonnement à la sous-matrice.

Exemple

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

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

$$\left(\begin{array}{r|r} 1 & 0 \\ \frac{88}{13} & -84 \end{array}\right) \xrightarrow{\times T_{2,1}(273)} \left(\begin{array}{r r} 1 & 0 \\ 0 & -84 \end{array}\right)$$

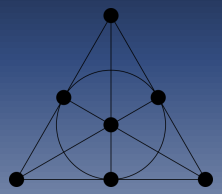


Corrolaire

En applicant le théorème précédent avec $\lambda = 1$, on obtient :

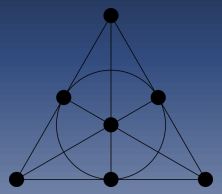
Corrolaire

SL(n, K) est engendré par les transvections.



Centralisateurs

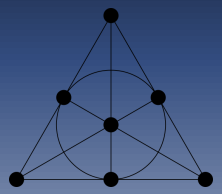
On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.



Centralisateurs

On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.

Théorème

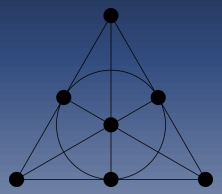


Centralisateurs

On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.

Théorème

- $\mathcal{Z}_{\mathrm{GL}(n,K)}(\mathrm{SL}(n,K)) = \mathcal{H}^*(n,K)$



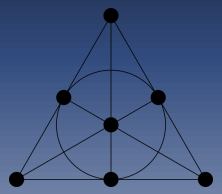
Centralisateurs

On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.

Théorème

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

Corollaire



Centralisateurs

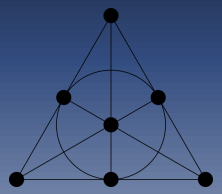
On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.

Théorème

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

Corollaire

- $\mathcal{Z}(\mathrm{GL}(n,K)) = \mathcal{H}^*(n,K)$



Centralisateurs

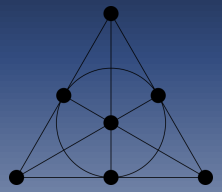
On peut montrer que si $M \in \mathfrak{M}_n(K)$ commute avec toutes les matrices de transvections, elle est multiple de l'identité.

Théorème

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

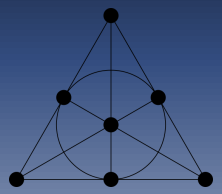
Corollaire

- $\mathcal{Z}(\mathrm{GL}(n,K)) = \mathcal{H}^*(n,K)$
- $\mathcal{Z}(\mathrm{SL}(n,K)) = \mathrm{S}\mathcal{H}^*(n,K)$



Centres des groupes projectifs

En applicant un raisonnement similaire mais sur des classes d'équivalences, on obtient :

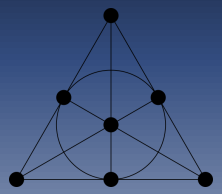


Centres des groupes projectifs

En applicant un raisonnement similaire mais sur des classes d'équivalences, on obtient :

Corollaire

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



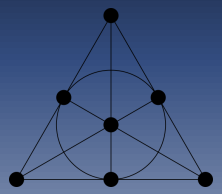
Centres des groupes projectifs

En applicant un raisonnement similaire mais sur des classes d'équivalences, on obtient :

Corollaire

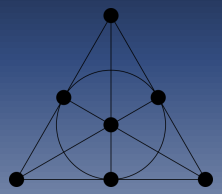
$\mathcal{Z}(\mathrm{PGL}(n,K))$ et $\mathcal{Z}(\mathrm{PSL}(n,K))$ sont réduits à l'élément neutre.

On a fait un pas vers la démonstration de la simplicité, mais nous en sommes encore loin. Nous allons nous intéresser de plus près aux groupes projectifs.



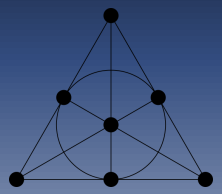
Notation vectorielle

Si E est un K-espace vectoriel de dimension n, alors l'espace vectoriel des endomorphismes de E est isomorphe à $\mathfrak{M}_n(K)$ pour une base fixée. Tous les groupes considérés peuvent alors s'écrire en notation vectorielle, par exemple, $\mathrm{GL}(n, K)$ devient $\mathrm{GL}_K(E)$.



Notation vectorielle

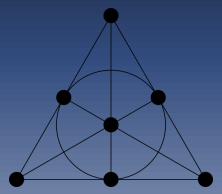
Si E est un K-espace vectoriel de dimension n, alors l'espace vectoriel des endomorphismes de E est isomorphe à $\mathfrak{M}_n(K)$ pour une base fixée. Tous les groupes considérés peuvent alors s'écrire en notation vectorielle, par exemple, $\mathrm{GL}(n, K)$ devient $\mathrm{GL}_K(E)$.
Déterminons les relations entre les différents groupes considérés.



Diagrammes commutatifs

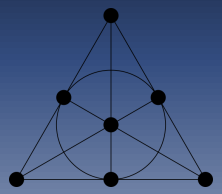
Par inclusions évidentes, on a :

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



Diagrammes commutatifs

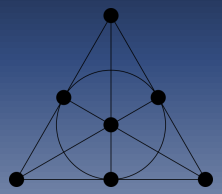
En notant ψ et ϕ les projections canoniques dans $\mathrm{PSL}(n, K)$ et $\mathrm{PGL}(n, K)$, on peut définir $\bar{j}$ qui à $\overline{M} \in \mathrm{PSL}(n, K)$ associe $\hat{M} \in \mathrm{PGL}(n, K)$. C'est une injection.



Diagrammes commutatifs

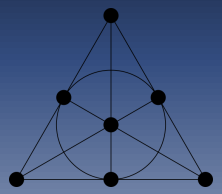
En notant ψ et ϕ les projections canoniques dans $\mathrm{PSL}(n, K)$ et $\mathrm{PGL}(n, K)$, on peut définir $\bar{j}$ qui à $\overline{M} \in \mathrm{PSL}(n, K)$ associe $\hat{M} \in \mathrm{PGL}(n, K)$. C'est une injection.

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



Diagrammes commutatifs

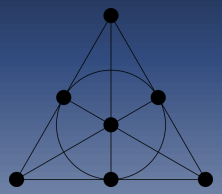
On note K^{*n} l'ensemble des λ^n pour $\lambda \in K^*$, alors on a immédiatement :



Diagrammes commutatifs

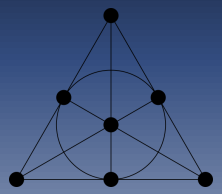
On note K^{*n} l'ensemble des λ^n pour $\lambda \in K^*$, alors on a immédiatement :

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



Diagrammes commutatifs

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 $\delta : \mathrm{PGL}_K(E) \to K^*/K^{*n}$ par $\delta(\phi(x)) = f(x)$, ce qui nous donne le diagramme suivant :

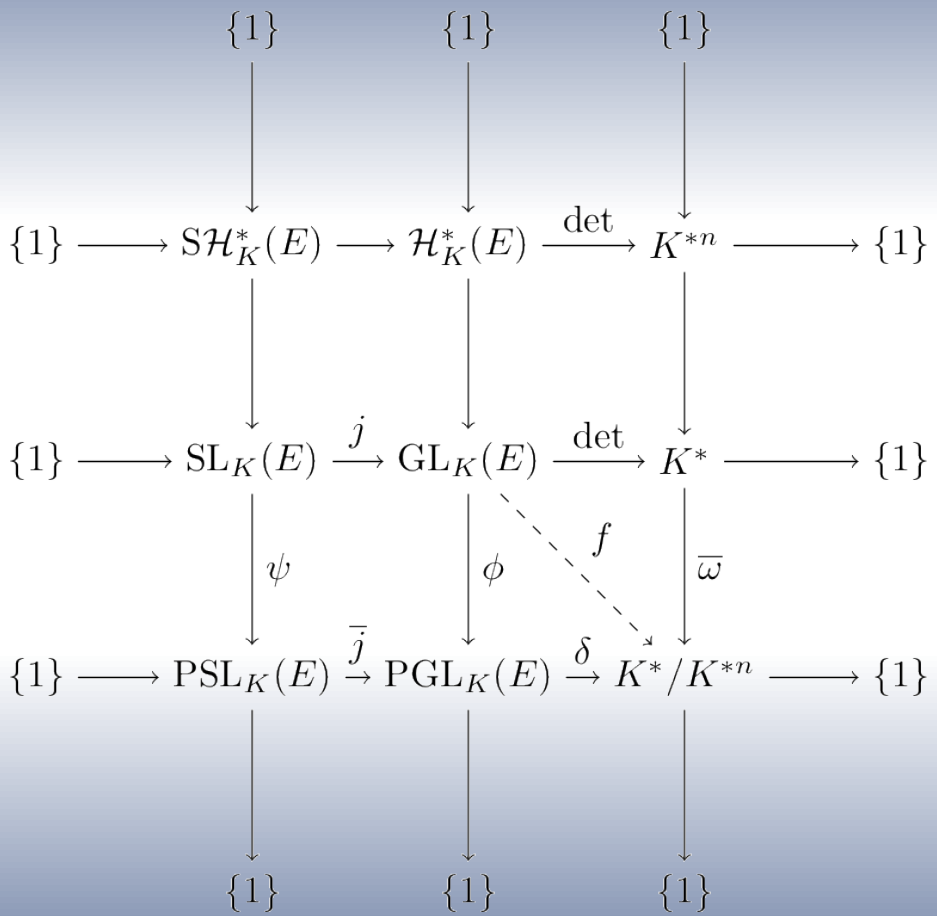


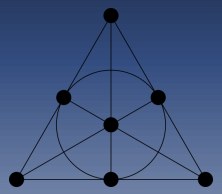
Diagrammes commutatifs

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 $\delta : \mathrm{PGL}_K(E) \to K^*/K^{*n}$ par $\delta(\phi(x)) = f(x)$, ce qui nous donne le diagramme suivant :

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

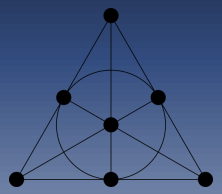
Diagramme commutatif exact





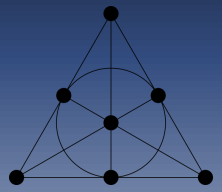
Transvections

Une transvection d'un espace vectoriel est un τ pour lequel il existe un hyperplan H, un vecteur v_0 non nul dans H et une forme linéaire ϕ de noyau H pour lequels $\tau(x) = x + \phi(x)v_0$.



Transvections

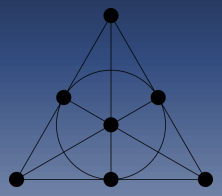
Une transvection d'un espace vectoriel est un τ pour lequel il existe un hyperplan H, un vecteur v_0 non nul dans H et une forme linéaire ϕ de noyau H pour lequels $\tau(x) = x + \phi(x)v_0$.
pour ϕ de noyau H et $v \in H$, on définit $\tau_{\phi,v}$ la transvection associée.



Transvections

Théorème

Il y a équivalence entre :

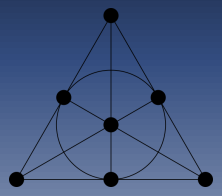


Transvections

Théorème

Il y a équivalence entre :

- τ est une transvection

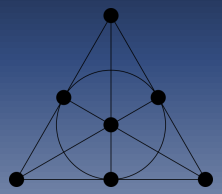


Transvections

Théorème

Il y a équivalence entre :

- τ est une transvection
- il existe une base dans laquelle sa matrice est de transvection

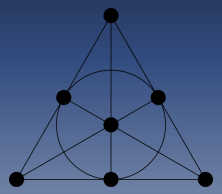


Transvections

Théorème

Il y a équivalence entre :

- τ est une transvection
- il existe une base dans laquelle sa matrice est de transvection
- il existe une base dans laquelle sa matrice est $T_{1,2}(1)$



Transvections

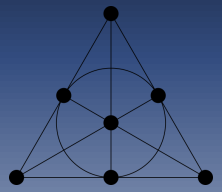
Théorème

Il y a équivalence entre :

- τ est une transvection
- il existe une base dans laquelle sa matrice est de transvection
- il existe une base dans laquelle sa matrice est $T_{1,2}(1)$

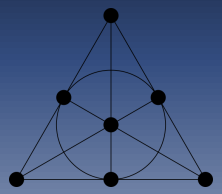
Pour $\tau(x) = x + \phi(x)v$, il suffit de fixer une base de H contenant v et de la compléter avec $e \in E$ en une base de E, alors la matrice de τ s'écrit :

$$\left(\begin{array}{ccccc|c} & & & & & 0 \\ & & I_{n-1} & & & \vdots \\ & & & & & 0 \\ \hline \phi(e) & 0 & \cdots & & 0 & 1 \end{array}\right)$$



Transvections

On déduit des résultats précédents :

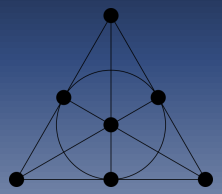


Transvections

On déduit des résultats précédents :

Corollaire

$\mathrm{SL}_K(E)$ est engendré par les transvections de E



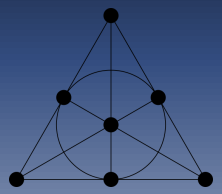
Transvections

On déduit des résultats précédents :

Corollaire

$\mathrm{SL}_K(E)$ est engendré par les transvections de E

Et comme toute matrice de transvections sont conjuguées à $T_{1,2}(1)$ dans $\mathrm{GL}(n, K)$, on obtient :



Transvections

On déduit des résultats précédents :

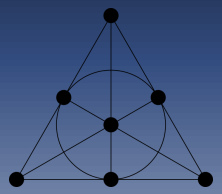
Corollaire

$\mathrm{SL}_K(E)$ est engendré par les transvections de E

Et comme toute matrice de transvections sont conjuguées à $T_{1,2}(1)$ dans $\mathrm{GL}(n, K)$, on obtient :

Corollaire

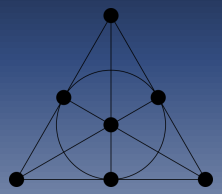
Deux transvections sont conjuguées dans $\mathrm{GL}_K(E)$, et une conjuguée d'une transvection est une transvection.



Transvections

Théorème

Soit H un hyperplan et $\tau \neq \mathrm{id}_E$, alors si $H \subset \ker(\tau - \mathrm{id}_E)$ et $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H$, τ est une transvection.

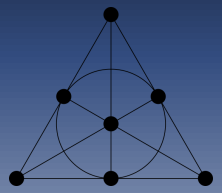


Transvections

Théorème

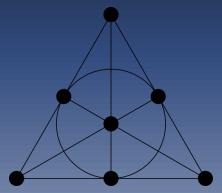
Soit H un hyperplan et $\tau \neq \mathrm{id}_E$, alors si $H \subset \ker(\tau - \mathrm{id}_E)$ et $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H$, τ est une transvection.

On fixe x_0 hors de H, alors $E = H \oplus Kx_0$, donc $\ker(\tau - \mathrm{id}_E) = H$. Posons $v_0 = \tau(x_0) - x_0 \neq 0$, on a $v_0 \in \mathrm{Im}(\tau - id_E) \subset H$. Soit ϕ la forme linéaire de noyau H telle que $\phi(x_0) = 1$, alors $\tau(x) = x + \phi(x)v_0$.



Conjugaisons dans $\mathrm{SL}_K(E)$

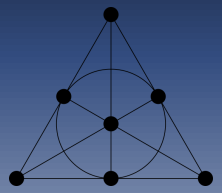
Théorème



Conjugaisons dans $\mathrm{SL}_K(E)$

Théorème

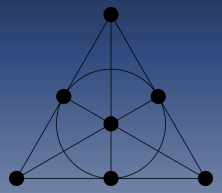
- pour $n \geqslant 3$, deux transvections sont conjuguées dans $\mathrm{SL}_K(E)$



Conjugaisons dans $\mathrm{SL}_K(E)$

Théorème

- pour $n \geqslant 3$, deux transvections sont conjuguées dans $\mathrm{SL}_K(E)$
- pour $n = 2$, l'ensemble $\mathcal{C}_T$ des classes de conjugaison dans $\mathrm{SL}_K(E)$ des transvections est en bijection avec K^*/K^{*2}, et plus précisément, si ρ parcourt une transversale de K^*/K^{*2}, alors $T_{1,2}(\rho)$ parcourt une transversale de $\mathcal{C}_T$.

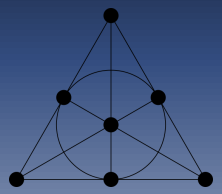


Conjugaisons dans $\mathrm{SL}_K(E)$

Théorème

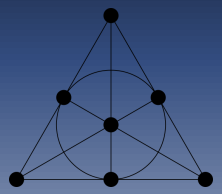
- pour $n \geqslant 3$, deux transvections sont conjuguées dans $\mathrm{SL}_K(E)$
- pour $n = 2$, l'ensemble $\mathcal{C}_T$ des classes de conjugaison dans $\mathrm{SL}_K(E)$ des transvections est en bijection avec K^*/K^{*2}, et plus précisément, si ρ parcourt une transversale de K^*/K^{*2}, alors $T_{1,2}(\rho)$ parcourt une transversale de $\mathcal{C}_T$.

Pour $n \geqslant 3$, soient τ et τ' deux transvections, $\mathfrak{B} = \{e_1, \ldots, e_n\}$ et $\mathfrak{B}' = \{e'_1, \ldots, e'_n\}$ les bases de E telles que $\mathrm{Mat}_{\mathfrak{B}}(\tau) = \mathrm{Mat}_{\mathfrak{B}'}(\tau') = T_{2,1}(1)$. On note $u_\rho \in \mathrm{GL}_K(E)$ telle que $u_\rho(e_i) = e'_i$ pour $i \neq n$ et $u_\rho(e_n) = \rho(e'_n)$. $u_\rho \tau u_\rho^{-1} = \tau'$ et $\det(u_\rho) = \rho \det(u_{1_K})$, en fixant $\rho = (\det(u_{1_k}))^{-1}$, τ et τ' sont conjuguées dans $\mathrm{SL}_K(E)$.



Conjugaisons quand $n = 2$

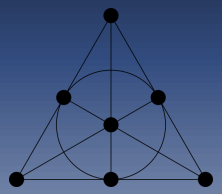
Soient ρ et ρ' dans K^*, alors :



Conjugaisons quand $n = 2$

Soient ρ et ρ' dans K^*, alors :

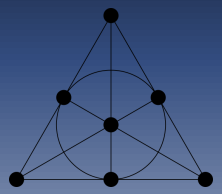
- Si $\rho = a^2\rho'$, alors $\begin{pmatrix} 1 & \rho' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \times \begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$



Conjugaisons quand $n = 2$

Soient ρ et ρ' dans K^*, alors :

- Si $\rho = a^2\rho'$, alors $\begin{pmatrix} 1 & \rho' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \times \begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$
- Si $\begin{pmatrix} 1 & \rho' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$, alors le calcul nous donne $\rho' = a^2\rho$.

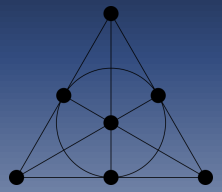


Conjugaisons quand $n = 2$

Soient ρ et ρ' dans K^*, alors :

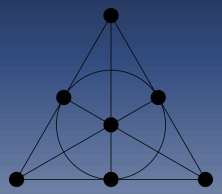
- Si $\rho = a^2\rho'$, alors $\begin{pmatrix} 1 & \rho' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \times \begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$
- Si $\begin{pmatrix} 1 & \rho' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$, alors le calcul nous donne $\rho' = a^2\rho$.

On a bien montré que $T_{1,2}(\rho)$ et $T_{1,2}(\rho')$ sont conjuguées dans $\mathrm{SL}(2, K)$ ssi $\frac{\rho}{\rho'} \in K^{*2}$.



Commutateurs

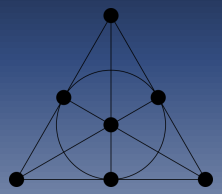
Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.



Commutateurs

Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.

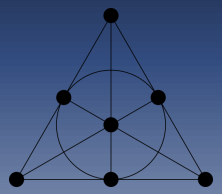
- $[G, G] \triangleleft G$



Commutateurs

Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.

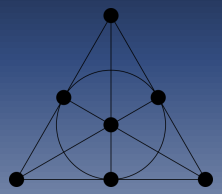
- $[G, G] \triangleleft G$
- $G/[G, G]$ abélien



Commutateurs

Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.

- $[G, G] \triangleleft G$
- $G/[G, G]$ abélien
- $H \triangleleft G$ et G/H abélien $\Rightarrow H \supset [G, G]$



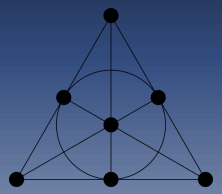
Commutateurs

Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.

- $[G, G] \triangleleft G$
- $G/[G, G]$ abélien
- $H \triangleleft G$ et G/H abélien $\Rightarrow H \supset [G, G]$

Théorème

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



Commutateurs

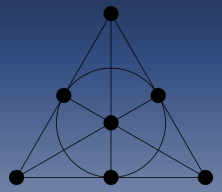
Le commutateur de G, noté $[G, G]$, est le groupe engendré par les $xyx^{-1}y^{-1}$ pour x et y dans G.

- $[G, G] \triangleleft G$
- $G/[G, G]$ abélien
- $H \triangleleft G$ et G/H abélien $\Rightarrow H \supset [G, G]$

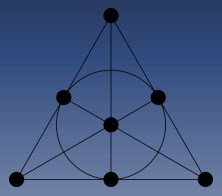
Théorème

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

La démonstration se fait en montrant que le commutateur contient toutes les transvections en se servant du fait qu'elles sont toutes conjuguées.

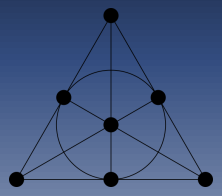


Les cas exclus



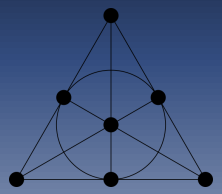
Les cas exclus

- $n = 2, K = \mathbb{F}_2$:



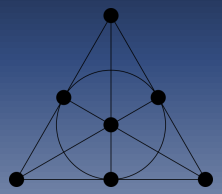
Les cas exclus

- $n = 2, K = \mathbb{F}_2$: $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2)$, et $\mathrm{GL}(2, \mathbb{F}_2)$ agit naturellement sur $K^2 \backslash 0$ qui est de cardinal 3 ; ainsi $\mathrm{GL}(2, \mathbb{F}_2)$ s'identifie à un sous-groupe de $\mathfrak{S}_3$. Comme $|\mathrm{GL}(2, \mathbb{F}_2)| = 6$, $\mathrm{GL}(2, \mathbb{F}_2) \cong \mathfrak{S}_3$, et $[\mathfrak{S}_3, \mathfrak{S}_3] = \mathfrak{A}_3$.



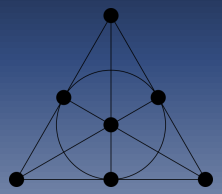
Les cas exclus

- $n = 2, K = \mathbb{F}_2$: $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2)$, et $\mathrm{GL}(2, \mathbb{F}_2)$ agit naturellement sur $K^2 \backslash 0$ qui est de cardinal 3 ; ainsi $\mathrm{GL}(2, \mathbb{F}_2)$ s'identifie à un sous-groupe de $\mathfrak{S}_3$. Comme $|\mathrm{GL}(2, \mathbb{F}_2)| = 6$, $\mathrm{GL}(2, \mathbb{F}_2) \cong \mathfrak{S}_3$, et $[\mathfrak{S}_3, \mathfrak{S}_3] = \mathfrak{A}_3$.
- $n = 2, K = \mathbb{F}_3$:



Les cas exclus

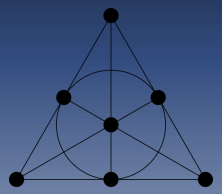
- $n = 2, K = \mathbb{F}_2$: $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2)$, et $\mathrm{GL}(2, \mathbb{F}_2)$ agit naturellement sur $K^2 \backslash 0$ qui est de cardinal 3 ; ainsi $\mathrm{GL}(2, \mathbb{F}_2)$ s'identifie à un sous-groupe de $\mathfrak{S}_3$. Comme $|\mathrm{GL}(2, \mathbb{F}_2)| = 6$, $\mathrm{GL}(2, \mathbb{F}_2) \cong \mathfrak{S}_3$, et $[\mathfrak{S}_3, \mathfrak{S}_3] = \mathfrak{A}_3$.
- $n = 2, K = \mathbb{F}_3$: On peut procéder similairement, ou procéder par recherche exhaustive. On trouve que $[\mathrm{SL}(2, \mathbb{F}_3), \mathrm{SL}(2, \mathbb{F}_3)]$ est un groupe quaternionique, donc d'ordre 8, alors que $\mathrm{SL}(2, \mathbb{F}_3)$ est d'ordre 24. En revanche, $[\mathrm{GL}(2, \mathbb{F}_3), \mathrm{GL}(2, \mathbb{F}_3)] = \mathrm{SL}(2, \mathbb{F}_3)$.



Simplicité des groupes projectifs

Théorème

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.

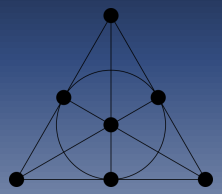


Simplicité des groupes projectifs

Théorème

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.

On démontre une propriété plus forte : si $G \triangleleft \mathrm{SL}_K(E)$, alors $G \subset S\mathcal{H}^*(n, K)$ ou $G = \mathrm{SL}_K(E)$. On fixe un tel G, et on suppose $G \not\subset S\mathcal{H}^*_K(E)$. On note $\mathcal{G}_1(E)$ l'ensemble des droites vectorielles de E. $S\mathcal{H}^*_K(E)$ est l'ensemble des $u \in \mathrm{GL}_K(E)$ laissant les droites de E invariantes, donc il existe u_0 dans G et deux droites D_1, D_2 telles que $u_0(D_1) = D_2$.

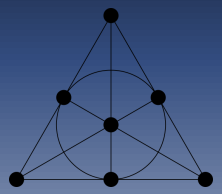


Simplicité des groupes projectifs

Théorème

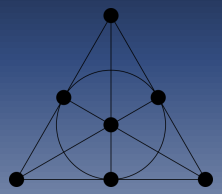
Hormis dans les cas $(n = 2, K = \mathbb{F}_2)$ et $(n = 2, K = \mathbb{F}_3)$,
le groupe $\mathrm{PSL}_K(E)$ est simple et non-abélien.

On démontre une propriété plus forte : si $G \triangleleft \mathrm{SL}_K(E)$, alors $G \subset S\mathcal{H}^*(n, K)$ ou $G = \mathrm{SL}_K(E)$. On fixe un tel G, et on suppose $G \not\subset S\mathcal{H}^*_K(E)$. On note $\mathcal{G}_1(E)$ l'ensemble des droites vectorielles de E. $S\mathcal{H}^*_K(E)$ est l'ensemble des $u \in \mathrm{GL}_K(E)$ laissant les droites de E invariantes, donc il existe u_0 dans G et deux droites D_1, D_2 telles que $u_0(D_1) = D_2$.
La démonstration se déroule en 5 temps :



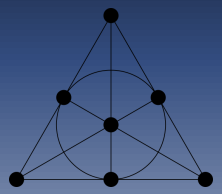
Démonstration

1. Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$ et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. On prouve $\Gamma_D \subset \Phi_D$ et que Γ_D est abélien.



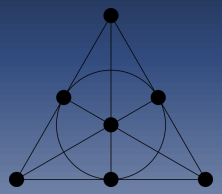
Démonstration

1. Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$ et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. On prouve $\Gamma_D \subset \Phi_D$ et que Γ_D est abélien.
2. On prouve que tous les Γ_D sont conjugués, de même pour les Φ_D.



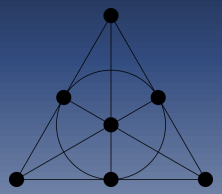
Démonstration

1. Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$ et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. On prouve $\Gamma_D \subset \Phi_D$ et que Γ_D est abélien.
2. On prouve que tous les Γ_D sont conjugués, de même pour les Φ_D.
3. On prouve la transitivité de G sur $\mathcal{G}_1(E)$, et on établit $G\Phi_{D_0} = \Phi_{D_0}G = \mathrm{SL}_K(E)$.



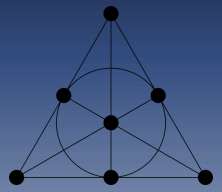
Démonstration

1. Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$ et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. On prouve $\Gamma_D \subset \Phi_D$ et que Γ_D est abélien.
2. On prouve que tous les Γ_D sont conjugués, de même pour les Φ_D.
3. On prouve la transitivité de G sur $\mathcal{G}_1(E)$, et on établit $G\Phi_{D_0} = \Phi_{D_0}G = \mathrm{SL}_K(E)$.
4. On établit $G\Gamma_{D_0} = \mathrm{SL}_K(E)$, donc $\mathrm{SL}_K(E)/G = G\Gamma_{D_0}/G \cong \Gamma_{D_0}/\Gamma_{D_0} \cap G$, et puisque Γ_{D_0} est abélien, $\mathrm{SL}_K(E)/G$ est abélien, et $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)] \subset G$, d'où $G = \mathrm{SL}_K(E)$.



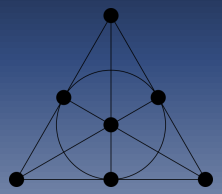
Démonstration

1. Pour $D \in \mathcal{G}_1(E)$, on pose $\Phi_D = \{u \in \mathrm{SL}_K(E) \mid u(D) = D\}$ et $\Gamma_D = \{u \in \mathrm{SL}_K(E) \mid \mathrm{Im}(u - \mathrm{id}_E) \subset D \text{ et } D \subset \ker(u - \mathrm{id}_E)\}$. On prouve $\Gamma_D \subset \Phi_D$ et que Γ_D est abélien.
2. On prouve que tous les Γ_D sont conjugués, de même pour les Φ_D.
3. On prouve la transitivité de G sur $\mathcal{G}_1(E)$, et on établit $G\Phi_{D_0} = \Phi_{D_0}G = \mathrm{SL}_K(E)$.
4. On établit $G\Gamma_{D_0} = \mathrm{SL}_K(E)$, donc $\mathrm{SL}_K(E)/G = G\Gamma_{D_0}/G \cong \Gamma_{D_0}/\Gamma_{D_0} \cap G$, et puisque Γ_{D_0} est abélien, $\mathrm{SL}_K(E)/G$ est abélien, et $[\mathrm{SL}_K(E), \mathrm{SL}_K(E)] \subset G$, d'où $G = \mathrm{SL}_K(E)$.
5. On trouve deux matrices qui ne commutent pas dans $\mathrm{PSL}_K(E)$: $U_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $V_2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.



Cas d'un corps fini

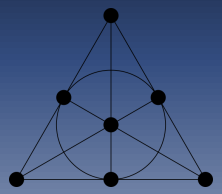
Déterminons le cardinal des groupes étudiés :



Cas d'un corps fini

Déterminons le cardinal des groupes étudiés :

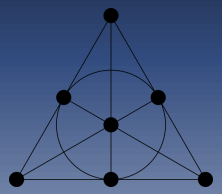
- le cardinal de $\mathrm{GL}(n, \mathbb{F}_q)$ est le nombre de matrices de rang n dans $\mathfrak{M}_n(\mathbb{F}_q)$, ou de n-uplet libre $(V_1, \ldots, V_n)$ de vecteurs de $\mathbb{F}_q^n$. V_1 est non-nul, il y a $q^n - 1$ choix pour V_1. $V_2 \notin \mathrm{Vect}(V_1)$, il y a $q^n - q$ choix pour V_2. Pour i fixé, il y a $q^n - q^{i-1}$ choix pour V_i ; on obtient donc :



Cas d'un corps fini

Déterminons le cardinal des groupes étudiés :

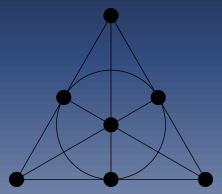
- le cardinal de $\mathrm{GL}(n, \mathbb{F}_q)$ est le nombre de matrices de rang n dans $\mathfrak{M}_n(\mathbb{F}_q)$, ou de n-uplet libre $(V_1, \ldots, V_n)$ de vecteurs de $\mathbb{F}_q^n$. V_1 est non-nul, il y a $q^n - 1$ choix pour V_1. $V_2 \notin \mathrm{Vect}(V_1)$, il y a $q^n - q$ choix pour V_2. Pour i fixé, il y a $q^n - q^{i-1}$ choix pour V_i ; on obtient donc : $|\mathrm{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = \mathcal{E}(n, q)$.



Cas d'un corps fini

Déterminons le cardinal des groupes étudiés :

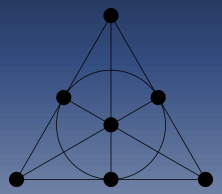
- le cardinal de $\mathrm{GL}(n, \mathbb{F}_q)$ est le nombre de matrices de rang n dans $\mathfrak{M}_n(\mathbb{F}_q)$, ou de n-uplet libre $(V_1, \ldots, V_n)$ de vecteurs de $\mathbb{F}_q^n$. V_1 est non-nul, il y a $q^n - 1$ choix pour V_1. $V_2 \notin \mathrm{Vect}(V_1)$, il y a $q^n - q$ choix pour V_2. Pour i fixé, il y a $q^n - q^{i-1}$ choix pour V_i ; on obtient donc : $|\mathrm{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = \mathcal{E}(n, q)$.
- $|\mathcal{H}^*(n, \mathbb{F}_q)| = |\mathbb{F}_q^*| = q - 1$, et comme $\mathrm{GL}(n, \mathbb{F}_q)/\mathrm{SL}(n, \mathbb{F}_q)1$ est isomorphe à l'ensemble des matrices de dilatations de déterminant non-nul, on obtient :



Cas d'un corps fini

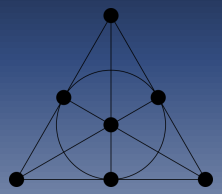
Déterminons le cardinal des groupes étudiés :

- le cardinal de $\mathrm{GL}(n, \mathbb{F}_q)$ est le nombre de matrices de rang n dans $\mathfrak{M}_n(\mathbb{F}_q)$, ou de n-uplet libre $(V_1, \ldots, V_n)$ de vecteurs de $\mathbb{F}_q^n$. V_1 est non-nul, il y a $q^n - 1$ choix pour V_1. $V_2 \notin \mathrm{Vect}(V_1)$, il y a $q^n - q$ choix pour V_2. Pour i fixé, il y a $q^n - q^{i-1}$ choix pour V_i ; on obtient donc : $|\mathrm{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) = \mathcal{E}(n, q)$.
- $|\mathcal{H}^*(n, \mathbb{F}_q)| = |\mathbb{F}_q^*| = q - 1$, et comme $\mathrm{GL}(n, \mathbb{F}_q)/\mathrm{SL}(n, \mathbb{F}_q)1$ est isomorphe à l'ensemble des matrices de dilatations de déterminant non-nul, on obtient : $|\mathrm{PGL}(n, \mathbb{F}_q)| = |\mathrm{SL}(n, \mathbb{F}_q)| = \frac{\mathcal{E}(n,q)}{(q-1)}$.



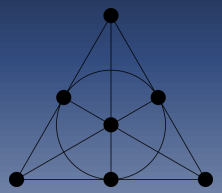
Cas d'un corps fini

$\mathbb{F}_q^*$ est un groupe cyclique, soit ω un générateur. L'ordre de ω^n est $e = \frac{q-1}{d}$, avec $d = \text{pgcd}(n, q-1)$, et $\omega^{nk} = 1_{\mathbb{F}_q} \Leftrightarrow k \equiv 0 \pmod{e}$.



Cas d'un corps fini

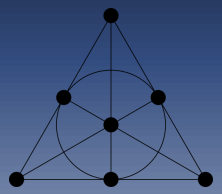
$\mathbb{F}_q^*$ est un groupe cyclique, soit ω un générateur. L'ordre de ω^n est $e = \frac{q-1}{d}$, avec $d = \text{pgcd}(n, q-1)$, et $\omega^{nk} = 1_{\mathbb{F}_q} \Leftrightarrow k \equiv 0 \pmod{e}$.
Soit $\xi \in \mathbb{F}_q^*$, alors $\xi = \omega^a$, et $\xi^n = 1_{\mathcal{F}_q}$ ssi $a \equiv 0 \pmod{e}$, donc l'ensemble des racines de l'unité est engendré par ω^e qui est d'ordre d. Cela nous donne $|\mathrm{S}\mathcal{H}^*(n, \mathcal{F}_q)| = d$, ou encore :



Cas d'un corps fini

$\mathbb{F}_q^*$ est un groupe cyclique, soit ω un générateur. L'ordre de ω^n est $e = \frac{q-1}{d}$, avec $d = \text{pgcd}(n, q-1)$, et $\omega^{nk} = 1_{\mathbb{F}_q} \Leftrightarrow k \equiv 0 \pmod{e}$.
Soit $\xi \in \mathbb{F}_q^*$, alors $\xi = \omega^a$, et $\xi^n = 1_{\mathcal{F}_q}$ ssi $a \equiv 0 \pmod{e}$, donc l'ensemble des racines de l'unité est engendré par ω^e qui est d'ordre d. Cela nous donne $|S\mathcal{H}^*(n, \mathcal{F}_q)| = d$, ou encore :

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

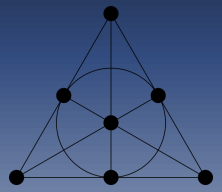


Cas d'un corps fini

$\mathbb{F}_q^*$ est un groupe cyclique, soit ω un générateur. L'ordre de ω^n est $e = \frac{q-1}{d}$, avec $d = \text{pgcd}(n, q-1)$, et $\omega^{nk} = 1_{\mathbb{F}_q} \Leftrightarrow k \equiv 0 \pmod{e}$.
Soit $\xi \in \mathbb{F}_q^*$, alors $\xi = \omega^a$, et $\xi^n = 1_{\mathcal{F}_q}$ ssi $a \equiv 0 \pmod{e}$, donc l'ensemble des racines de l'unité est engendré par ω^e qui est d'ordre d. Cela nous donne $|S\mathcal{H}^*(n, \mathcal{F}_q)| = d$, ou encore :

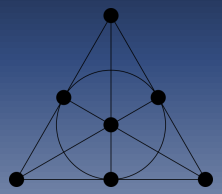
$$|\,\mathrm{PSL}(n, \mathbb{F}_q)| = \frac{|\,\mathrm{SL}(n, \mathbb{F}_q)|}{|S\mathcal{H}^*(n, \mathbb{F}_q)|} = \frac{\mathcal{E}(n, q)}{d(q-1)}$$

On a alors $|\,\mathrm{PSL}(2, \mathbb{F}_7)| = |\,\mathrm{PSL}(3, \mathbb{F}_2)| = 168$: étudions plus précisément ces groupes.



$\mathcal{S}_3$-système

Un $\mathcal{S}_3$-système est composé d'un ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes :

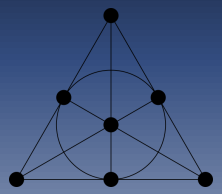


$\mathcal{S}_3$-système

Un $\mathcal{S}_3$-système est composé d'un ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes :

$(1,2)$-incidence

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

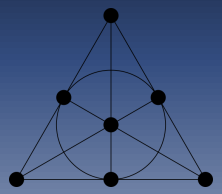


$\mathcal{S}_3$-système

Un $\mathcal{S}_3$-système est composé d'un ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes :

$(1,2)$-incidence

1. Soient D_1 et $D_2 \in \mathcal{D}$ distincts, alors $D_1 \cap D_2$ est un singleton.
2. Soient A_1 et $A_2 \in S$ distincts, alors $\exists! A_3 \in S$ tel que $\{A_1, A_2, A_3\} \in \mathcal{D}$.

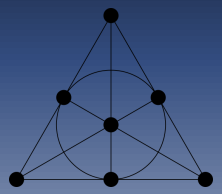


$\mathcal{S}_3$-système

Un $\mathcal{S}_3$-système est composé d'un ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes :

$(1,2)$-incidence

1. Soient D_1 et $D_2 \in \mathcal{D}$ distincts, alors $D_1 \cap D_2$ est un singleton.
2. Soient A_1 et $A_2 \in S$ distincts, alors $\exists! A_3 \in S$ tel que $\{A_1, A_2, A_3\} \in \mathcal{D}$.
3. $|\mathcal{D} \geqslant 2|$.



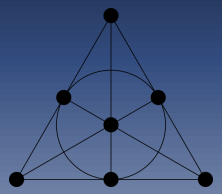
$\mathcal{S}_3$-système

Un $\mathcal{S}_3$-système est composé d'un ensemble fini non-vide S associé à un ensemble $\mathcal{D}$ de 3-parties de S vérifiant les conditions suivantes :

$(1,2)$-incidence

1. Soient D_1 et $D_2 \in \mathcal{D}$ distincts, alors $D_1 \cap D_2$ est un singleton.
2. Soient A_1 et $A_2 \in S$ distincts, alors $\exists! A_3 \in S$ tel que $\{A_1, A_2, A_3\} \in \mathcal{D}$.
3. $|\mathcal{D} \geqslant 2|$.

Soit E un $\mathbb{F}_2$-espace vectoriel de dimension 3. Posons $S = E \backslash \{0\}$ et $\mathcal{D}$ l'ensemble des plans de E privés de 0. Alors $(S, \mathcal{D})$ est un $\mathcal{S}_3$-système.



Représentation d'un $\mathcal{S}_3$-système

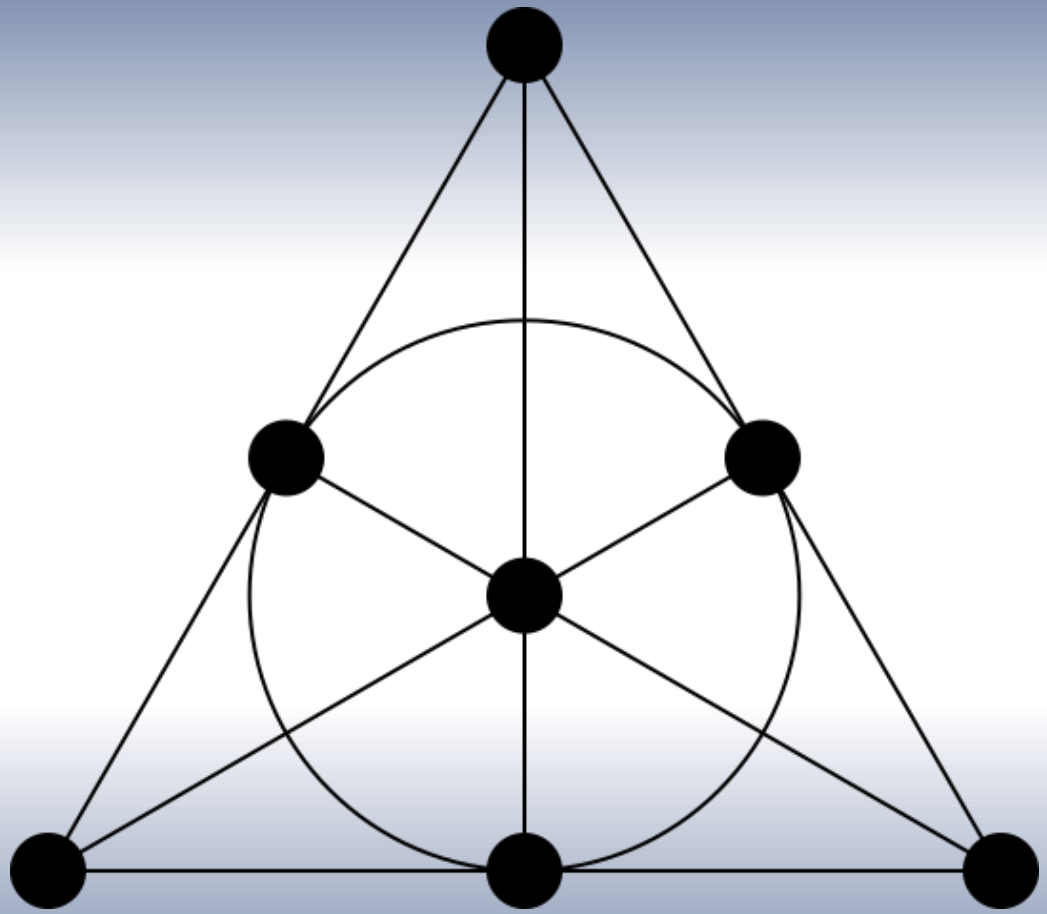
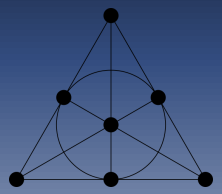
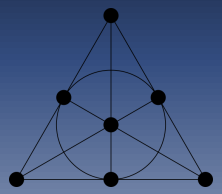


Figure – Les points représentent S, les lignes $\mathcal{D}$



$\mathcal{S}_3$-système

On peut construire un $\mathcal{S}_3$-système à partir d'un espace vectoriel, on va montrer que tous les $\mathcal{S}_3$-système sont de cette forme :

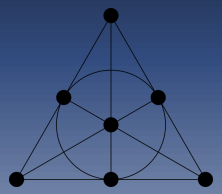


$\mathcal{S}_3$-système

On peut construire un $\mathcal{S}_3$-système à partir d'un espace vectoriel, on va montrer que tous les $\mathcal{S}_3$-système sont de cette forme :

Théorème

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 $\dim_{\mathbb{F}_2}(E) = 3$, $0_E = \underline{O}$.



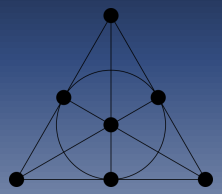
$\mathcal{S}_3$-système

On peut construire un $\mathcal{S}_3$-système à partir d'un espace vectoriel, on va montrer que tous les $\mathcal{S}_3$-système sont de cette forme :

Théorème

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 $\dim_{\mathbb{F}_2}(E) = 3$, $0_E = \underline{O}$.

On définit une loi d'addition pour laquelle $\underline{O}$ est l'élément neutre, et $-x = x$. Pour $x, y \in S$, on sait qu'il existe un z tel que $\{x, y, z\} \in \mathcal{D}$, définissons $x + y = z$.



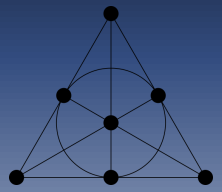
$\mathcal{S}_3$-système

On peut construire un $\mathcal{S}_3$-système à partir d'un espace vectoriel, on va montrer que tous les $\mathcal{S}_3$-système sont de cette forme :

Théorème

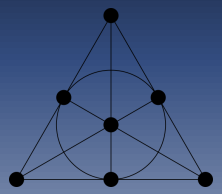
Soit $(S, \mathcal{D})$ un $\mathcal{S}_3$-système, et soit $\underline{O} \notin S$, alors il existe une unique structure de $\mathbb{F}_2$-espace vectoriel sur $E = S \cup \{\underline{O}\}$ telle que $\dim_{\mathbb{F}_2}(E) = 3$, $0_E = \underline{O}$.

On définit une loi d'addition pour laquelle $\underline{O}$ est l'élément neutre, et $-x = x$. Pour $x, y \in S$, on sait qu'il existe un z tel que $\{x, y, z\} \in \mathcal{D}$, définissons $x + y = z$. Cette loi est commutative, il nous faut vérifier son associativité.



Associativité

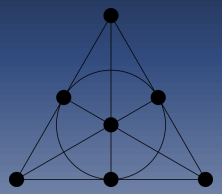
Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.



Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

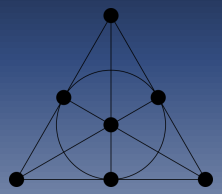
- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$



Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

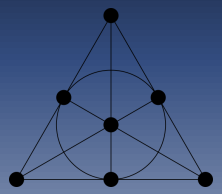
- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$
- On pose $y + z = x_1 \neq x$, on veut montrer $x + x_1 = z_2 \Leftrightarrow \{x, x_1, z_2\} \in \mathcal{D}$



Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

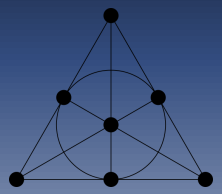
- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$
- On pose $y + z = x_1 \neq x$, on veut montrer $x + x_1 = z_2 \Leftrightarrow \{x, x_1, z_2\} \in \mathcal{D}$
- $\{z, z_1, z_2\} \cap \{y, z, x_1\} = \{z\}$ et $\{y, z, x_1\} \cap \{x, y, z_1\} = \{y\}$



Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$
- On pose $y + z = x_1 \neq x$, on veut montrer $x + x_1 = z_2 \Leftrightarrow \{x, x_1, z_2\} \in \mathcal{D}$
- $\{z, z_1, z_2\} \cap \{y, z, x_1\} = \{z\}$ et $\{y, z, x_1\} \cap \{x, y, z_1\} = \{y\}$
- Soit D l'élément de $\mathcal{D}$ contenant x et x_1, et $D' = \{z, z_1, z_2\}$. Ils se rencontrent en un seul point, qui est forcément z_2, donc $x + x_1 = z_2$.

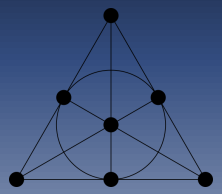


Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$
- On pose $y + z = x_1 \neq x$, on veut montrer $x + x_1 = z_2 \Leftrightarrow \{x, x_1, z_2\} \in \mathcal{D}$
- $\{z, z_1, z_2\} \cap \{y, z, x_1\} = \{z\}$ et $\{y, z, x_1\} \cap \{x, y, z_1\} = \{y\}$
- Soit D l'élément de $\mathcal{D}$ contenant x et x_1, et $D' = \{z, z_1, z_2\}$. Ils se rencontrent en un seul point, qui est forcément z_2, donc $x + x_1 = z_2$.

Pour achever la construction, on définit la loi externe de manière naturelle : $0 \cdot x = \underline{O}$ et $1 \cdot x = x$.

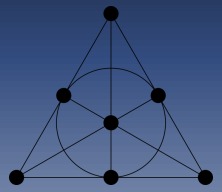


Associativité

Le seul cas problématique est $x, y, z \in S$ distincts avec $\{x, y, z\} \notin \mathcal{D}$.

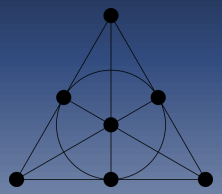
- On pose $x + y = z_1 \neq z$, et $z_1 + z = z_2$: $(x + y) + z = z_2$
- On pose $y + z = x_1 \neq x$, on veut montrer $x + x_1 = z_2 \Leftrightarrow \{x, x_1, z_2\} \in \mathcal{D}$
- $\{z, z_1, z_2\} \cap \{y, z, x_1\} = \{z\}$ et $\{y, z, x_1\} \cap \{x, y, z_1\} = \{y\}$
- Soit D l'élément de $\mathcal{D}$ contenant x et x_1, et $D' = \{z, z_1, z_2\}$. Ils se rencontrent en un seul point, qui est forcément z_2, donc $x + x_1 = z_2$.

Pour achever la construction, on définit la loi externe de manière naturelle : $0 \cdot x = \underline{O}$ et $1 \cdot x = x$.
Pour $D \in \mathcal{D}$, $D \cup \{\underline{O}\}$ est un plan de E. On sait qu'il y a au moins 2 plans, mais qu'il n'y a pas deux plans qui ne se croisent qu'en $\underline{O}$, donc $\dim_{\mathbb{F}_2}(E) = 3$.



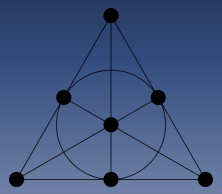
Automorphismes

Un isomorphisme entre deux $\mathcal{S}_3$-système $(S, \mathcal{D})$ et $(S', \mathcal{D}')$ est une bijection entre S et S' qui induit une bijection entre $\mathcal{D}$ et $\mathcal{D}'$.



Automorphismes

Un isomorphisme entre deux $\mathcal{S}_3$-système $(S, \mathcal{D})$ et $(S', \mathcal{D}')$ est une bijection entre S et S' qui induit une bijection entre $\mathcal{D}$ et $\mathcal{D}'$.
Les automorphismes d'un $\mathcal{S}_3$-système forment un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$, et correspondent exactement aux automorphismes de E, donc à $\mathrm{GL}_{\mathbb{F}_2}(E) = \mathrm{PSL}_{\mathbb{F}_2}(E) = \mathrm{PSL}(3, \mathbb{F}_2)$.

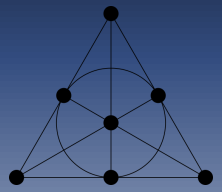


Automorphismes

Un isomorphisme entre deux $\mathcal{S}_3$-système $(S, \mathcal{D})$ et $(S', \mathcal{D}')$ est une bijection entre S et S' qui induit une bijection entre $\mathcal{D}$ et $\mathcal{D}'$.
Les automorphismes d'un $\mathcal{S}_3$-système forment un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$, et correspondent exactement aux automorphismes de E, donc à $\mathrm{GL}_{\mathbb{F}_2}(E) = \mathrm{PSL}_{\mathbb{F}_2}(E) = \mathrm{PSL}(3, \mathbb{F}_2)$.

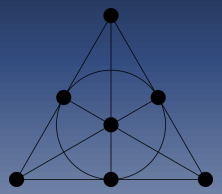
Théorème

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.



Action sur un ensemble à 7 points

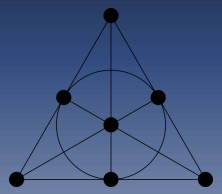
Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.



Action sur un ensemble à 7 points

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.

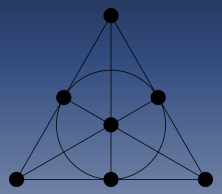
- $\ker(\Phi)$ est un sous-groupe distingué de G, alors $\ker(\Phi) = \{e\}$ car G est simple et l'action est transitive. On peut voir G comme un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$.



Action sur un ensemble à 7 points

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.

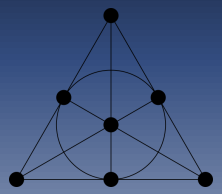
- $\ker(\Phi)$ est un sous-groupe distingué de G, alors $\ker(\Phi) = \{e\}$ car G est simple et l'action est transitive. On peut voir G comme un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$.
- $G \in \mathfrak{A}_7$ par l'étude de la signature.



Action sur un ensemble à 7 points

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.

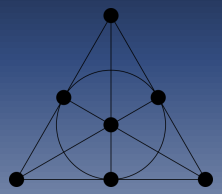
- $\ker(\Phi)$ est un sous-groupe distingué de G, alors $\ker(\Phi) = \{e\}$ car G est simple et l'action est transitive. On peut voir G comme un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$.
- $G \in \mathfrak{A}_7$ par l'étude de la signature.
- G contient un élément d'ordre 7 car $7|168$, c'est un 7-cycle.



Action sur un ensemble à 7 points

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.

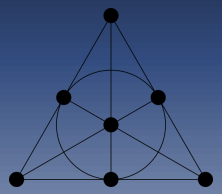
- $\ker(\Phi)$ est un sous-groupe distingué de G, alors $\ker(\Phi) = \{e\}$ car G est simple et l'action est transitive. On peut voir G comme un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$.
- $G \in \mathfrak{A}_7$ par l'étude de la signature.
- G contient un élément d'ordre 7 car $7|168$, c'est un 7-cycle.
- G ne contient pas de 3-cycle, car $\mathfrak{A}_7$, de cardinal 2520, est engendré par n'importe quel couple d'un 3-cycle et d'un 7-cycle.



Action sur un ensemble à 7 points

Soit G un groupe simple d'ordre 168, et une action à gauche transitive de G sur S à 7 éléments. Soit Φ associée à cette action.

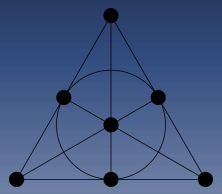
- $\ker(\Phi)$ est un sous-groupe distingué de G, alors $\ker(\Phi) = \{e\}$ car G est simple et l'action est transitive. On peut voir G comme un sous-groupe de $\mathfrak{S}_S \cong \mathfrak{S}_7$.
- $G \in \mathfrak{A}_7$ par l'étude de la signature.
- G contient un élément d'ordre 7 car $7|168$, c'est un 7-cycle.
- G ne contient pas de 3-cycle, car $\mathfrak{A}_7$, de cardinal 2520, est engendré par n'importe quel couple d'un 3-cycle et d'un 7-cycle.
- G contient un élément d'ordre 2. C'est une bitransposition. Notamment, elle a 3 points fixes dans S.



Construction d'un $\mathcal{S}_3$-système

Théorème

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

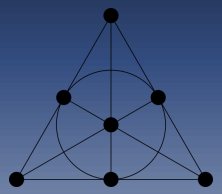


Construction d'un $\mathcal{S}_3$-système

Théorème

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

- Soient a et b distincts dans S ; G_a et G_b, leurs stabilisateurs, sont conjugués dans G et de cardinal 24.

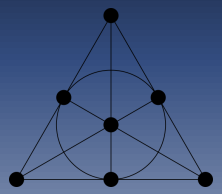


Construction d'un $\mathcal{S}_3$-système

Théorème

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

- Soient a et b distincts dans S ; G_a et G_b, leurs stabilisateurs, sont conjugués dans G et de cardinal 24.
- Soit $\mathcal{E} = S \backslash \{a, b\}$ et $H = G_a \cap G_b$, H agit fidèlement sur $\mathcal{E}$ et s'identifie à un sous-groupe de $\mathfrak{S}_\mathcal{E}$.

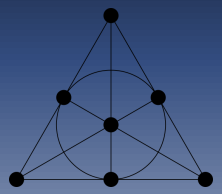


Construction d'un $\mathcal{S}_3$-système

Théorème

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

- Soient a et b distincts dans S ; G_a et G_b, leurs stabilisateurs, sont conjugués dans G et de cardinal 24.
- Soit $\mathcal{E} = S \backslash \{a, b\}$ et $H = G_a \cap G_b$, H agit fidèlement sur $\mathcal{E}$ et s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{E}}$.
- Cette action n'est pas transitive, car $|\mathcal{E}| = 5 \not| 168 = |G|$. Si elle n'admet pas de point fixe, alors elle a deux orbites, dont une de cardinal 3 sur laquelle elle induit un 3-cycle, ce qui est impossible.

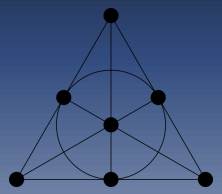


Construction d'un $\mathcal{S}_3$-système

Théorème

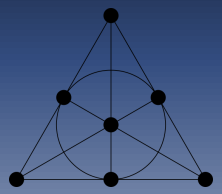
Soit $\mathcal{D}$ l'ensemble des 3-parties de S fixées par les bitranspositions de G. Alors $(S, \mathcal{D})$ est un $\mathcal{S}_3$-système.

- Soient a et b distincts dans S ; G_a et G_b, leurs stabilisateurs, sont conjugués dans G et de cardinal 24.
- Soit $\mathcal{E} = S \backslash \{a, b\}$ et $H = G_a \cap G_b$, H agit fidèlement sur $\mathcal{E}$ et s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{E}}$.
- Cette action n'est pas transitive, car $|\mathcal{E}| = 5 \not| 168 = |G|$. Si elle n'admet pas de point fixe, alors elle a deux orbites, dont une de cardinal 3 sur laquelle elle induit un 3-cycle, ce qui est impossible.
- Ainsi cette action admet un point fixe c.



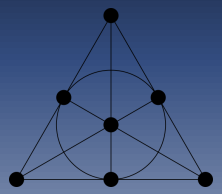
Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.



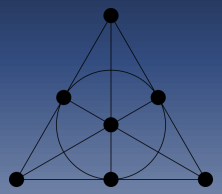
Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.



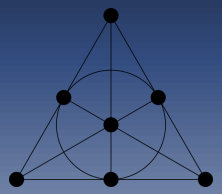
Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.



Construction d'un $\mathcal{S}_3$-système

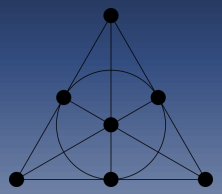
- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.
- Ainsi pour tout a, b dans S, il existe un unique c tel que $\{a, b, c\} \in \mathcal{D}$.



Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.
- Ainsi pour tout a, b dans S, il existe un unique c tel que $\{a, b, c\} \in \mathcal{D}$.

Comme $|S| = 7$, on vérifie $|\mathcal{D}| \geqslant 2$. Enfin :

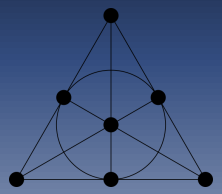


Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.
- Ainsi pour tout a, b dans S, il existe un unique c tel que $\{a, b, c\} \in \mathcal{D}$.

Comme $|S| = 7$, on vérifie $|\mathcal{D}| \geqslant 2$. Enfin :

- Deux éléments distincts de $\mathcal{D}$ se croisent en au plus 1 point.

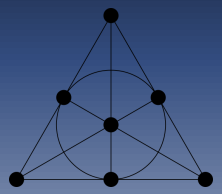


Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.
- Ainsi pour tout a, b dans S, il existe un unique c tel que $\{a, b, c\} \in \mathcal{D}$.

Comme $|S| = 7$, on vérifie $|\mathcal{D}| \geqslant 2$. Enfin :

- Deux éléments distincts de $\mathcal{D}$ se croisent en au plus 1 point.
- Si u et v sont deux bitranspositions dont les ensembles de points fixes soint disjoints, alors $(uv)^2$ est un 3-cycle, ce qui est impossible.

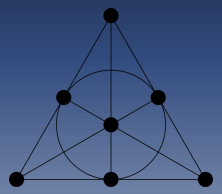


Construction d'un $\mathcal{S}_3$-système

- H est formé des permutations paires de $\mathcal{E}\backslash\{c\}$, donc de 4 éléments.
- Il ne contient pas de 3-cycle, donc il ne contient que des bitranspositions laisant a, b, et c fixes.
- Il n'est pas réduit à l'identité, car sinon G contiendrait au moins 24^2 éléments.
- Ainsi pour tout a, b dans S, il existe un unique c tel que $\{a, b, c\} \in \mathcal{D}$.

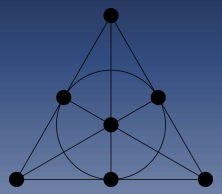
Comme $|S| = 7$, on vérifie $|\mathcal{D}| \geqslant 2$. Enfin :

- Deux éléments distincts de $\mathcal{D}$ se croisent en au plus 1 point.
- Si u et v sont deux bitranspositions dont les ensembles de points fixes soint disjoints, alors $(uv)^2$ est un 3-cycle, ce qui est impossible.



Isomorphisme

$(S, \mathcal{D})$ est un $\mathcal{S}_3$-système, et soient $g \in G$ et $D \in \mathcal{D}$. Il existe une bitransposition $u \in G$ dont l'ensemble des points fixes est D, alors gug^{-1} est une bistransposition de G dont l'ensemble des points fixes est $g(D)$, donc $g(D) \in \mathcal{D}$.

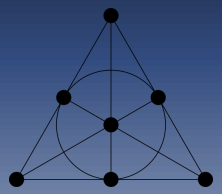


Isomorphisme

$(S, \mathcal{D})$ est un $\mathcal{S}_3$-système, et soient $g \in G$ et $D \in \mathcal{D}$. Il existe une bitransposition $u \in G$ dont l'ensemble des points fixes est D, alors gug^{-1} est une bistransposition de G dont l'ensemble des points fixes est $g(D)$, donc $g(D) \in \mathcal{D}$.

Théorème

Si un groupe simple d'ordre 168 agit transitivement sur un ensemble à 7 éléments, alors il est isomorphe à $PSL(3, \mathbb{F}_2)$.



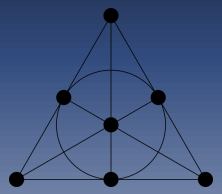
Isomorphisme

$(S, \mathcal{D})$ est un $\mathcal{S}_3$-système, et soient $g \in G$ et $D \in \mathcal{D}$. Il existe une bitransposition $u \in G$ dont l'ensemble des points fixes est D, alors gug^{-1} est une bistransposition de G dont l'ensemble des points fixes est $g(D)$, donc $g(D) \in \mathcal{D}$.

Théorème

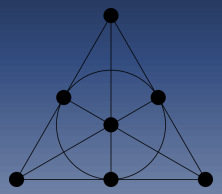
Si un groupe simple d'ordre 168 agit transitivement sur un ensemble à 7 éléments, alors il est isomorphe à $PSL(3, \mathbb{F}_2)$.

Il nous suffit maintenant de trouver une telle action pour tout groupe simple d'ordre 168. À cet effet, on étudiera les p-Sylow d'un tel groupe G.



7-Sylow

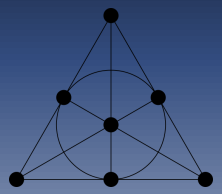
On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.



7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

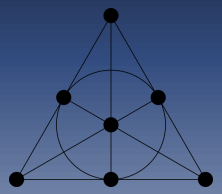
- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.



7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

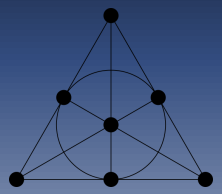
- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.
- L'intersection de deux 7-Sylow est $\{1_G\}$, donc $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$.



7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

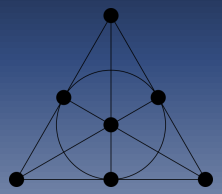
- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.
- L'intersection de deux 7-Sylow est $\{1_G\}$, donc $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$.
- L'action de G sur $\mathcal{S}_7$ est transitive, donc G s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{S}_7} \cong \mathfrak{S}_8$. L'étude du noyau de la signature montre même $G \subset \mathfrak{A}_8$.



7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

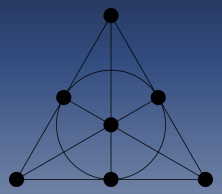
- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.
- L'intersection de deux 7-Sylow est $\{1_G\}$, donc $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$.
- L'action de G sur $\mathcal{S}_7$ est transitive, donc G s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{S}_7} \cong \mathfrak{S}_8$. L'étude du noyau de la signature montre même $G \subset \mathfrak{A}_8$.
- $\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$, le normalisateur d'un 7-Sylow H dans G, est de cardinal 21. Un élément d'ordre 21 devrait contenir dans sa décomposition en cycles disjoints au moins un 3-cycle et un 7-cycle, ce qui est impossible dans $\mathfrak{A}_8$.



7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

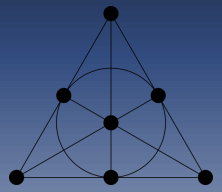
- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.
- L'intersection de deux 7-Sylow est $\{1_G\}$, donc $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$.
- L'action de G sur $\mathcal{S}_7$ est transitive, donc G s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{S}_7} \cong \mathfrak{S}_8$. L'étude du noyau de la signature montre même $G \subset \mathfrak{A}_8$.
- $\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$, le normalisateur d'un 7-Sylow H dans G, est de cardinal 21. Un élément d'ordre 21 devrait contenir dans sa décomposition en cycles disjoints au moins un 3-cycle et un 7-cycle, ce qui est impossible dans $\mathfrak{A}_8$.
- $\mathcal{N}_G(H)$ ne contient qu'un seul sous-groupe d'ordre 7 (7-Sylow), et donc les éléments qui commutent avec les éléments d'ordre 7 sont d'ordre 3 ou 7.



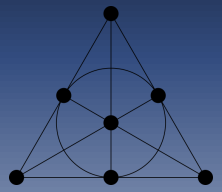
7-Sylow

On notera $\mathcal{S}_p$ l'ensemble des p-Sylow de G et $\mathcal{O}_i$ l'ensemble des éléments d'ordre i.

- $|\mathcal{S}_7| \equiv 1 \pmod 7$, et $|\mathcal{S}_7| \big| 24$. Comme G est simple, $|\mathcal{S}_7| > 1$, donc $|\mathcal{S}_7| = 8$.
- L'intersection de deux 7-Sylow est $\{1_G\}$, donc $|\mathcal{O}_7| = |\mathcal{S}_7| \cdot (7-1) = 48$.
- L'action de G sur $\mathcal{S}_7$ est transitive, donc G s'identifie à un sous-groupe de $\mathfrak{S}_{\mathcal{S}_7} \cong \mathfrak{S}_8$. L'étude du noyau de la signature montre même $G \subset \mathfrak{A}_8$.
- $\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$, le normalisateur d'un 7-Sylow H dans G, est de cardinal 21. Un élément d'ordre 21 devrait contenir dans sa décomposition en cycles disjoints au moins un 3-cycle et un 7-cycle, ce qui est impossible dans $\mathfrak{A}_8$.
- $\mathcal{N}_G(H)$ ne contient qu'un seul sous-groupe d'ordre 7 (7-Sylow), et donc les éléments qui commutent avec les éléments d'ordre 7 sont d'ordre 3 ou 7.
- L'intersection de deux normalisateurs est un 3-Sylow de G. Ceci implique $|\mathcal{O}_3| \geqslant 26$ et que tous les $\mathcal{N}_G(H)$ sont distincts.

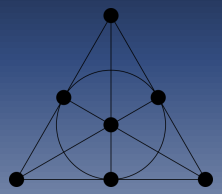


3-Sylow



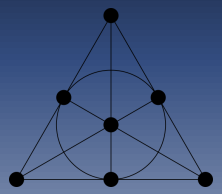
3-Sylow

- Le nombre de 3-Sylow est 4, 7, ou 28.



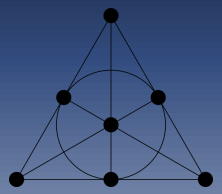
3-Sylow

- Le nombre de 3-Sylow est 4, 7, ou 28.
- $|\mathcal{O}_3| = 2|\mathcal{S}_3|$. Comme $|\mathcal{O}_3| \geqslant 26$, on a $|\mathcal{S}_3| = 28$ et $|\mathcal{O}_3| = 56$.



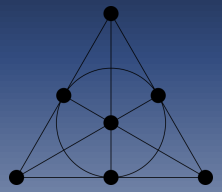
3-Sylow

- Le nombre de 3-Sylow est 4, 7, ou 28.
- $|\mathcal{O}_3| = 2|\mathcal{S}_3|$. Comme $|\mathcal{O}_3| \geqslant 26$, on a $|\mathcal{S}_3| = 28$ et $|\mathcal{O}_3| = 56$.
- Pour $H \in \mathcal{S}_3$, le normalisateur $\mathcal{N}_G(H)$ est de cardinal 6.
- S'il existe x dans G d'ordre 6, alors x^2 engendre un 3-Sylow H, et $\mathcal{N}_G(H)$ est cyclique, engendré par x. Alors tous les $\mathcal{N}_G(H)$ sont cycliques, et il existe au moins 56 éléments d'ordre 6, en plus des 56 d'ordre 3 et des 48 d'ordre 7. Alors G ne contient que 7 éléments d'ordre 2, donc un seul 2-Sylow, ce qui est impossible par simplicité de G.

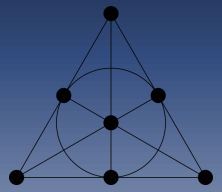


3-Sylow

- Le nombre de 3-Sylow est 4, 7, ou 28.
- $|\mathcal{O}_3| = 2|\mathcal{S}_3|$. Comme $|\mathcal{O}_3| \geqslant 26$, on a $|\mathcal{S}_3| = 28$ et $|\mathcal{O}_3| = 56$.
- Pour $H \in \mathcal{S}_3$, le normalisateur $\mathcal{N}_G(H)$ est de cardinal 6.
- S'il existe x dans G d'ordre 6, alors x^2 engendre un 3-Sylow H, et $\mathcal{N}_G(H)$ est cyclique, engendré par x. Alors tous les $\mathcal{N}_G(H)$ sont cycliques, et il existe au moins 56 éléments d'ordre 6, en plus des 56 d'ordre 3 et des 48 d'ordre 7. Alors G ne contient que 7 éléments d'ordre 2, donc un seul 2-Sylow, ce qui est impossible par simplicité de G.
- Il n'y a pas d'élément d'ordre 6 dans G, et les $\mathcal{N}_G(H)$ sont isomorphes à $\mathfrak{S}_3$. Aucun élément d'ordre 2 ne permute avec un élément d'ordre 3.

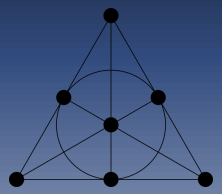


2-Sylow



2-Sylow

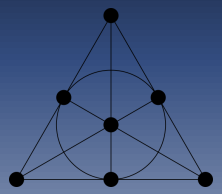
Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84



2-Sylow

Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84

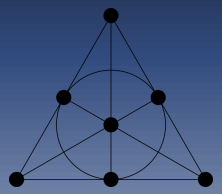
- On sait qu'ils ne peuvent pas être d'ordre 6, ni a fortiori d'ordre 12, 42 ou 84.



2-Sylow

Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84

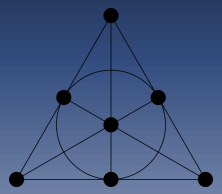
- On sait qu'ils ne peuvent pas être d'ordre 6, ni a fortiori d'ordre 12, 42 ou 84.
- Un élément d'ordre 8 serait un 8-cycle, qui est une permutation impaire. Il n'y a donc ni élément d'ordre 8, ni d'ordre 24 ou 56.



2-Sylow

Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84

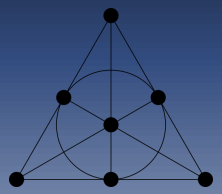
- On sait qu'ils ne peuvent pas être d'ordre 6, ni a fortiori d'ordre 12, 42 ou 84.
- Un élément d'ordre 8 serait un 8-cycle, qui est une permutation impaire. Il n'y a donc ni élément d'ordre 8, ni d'ordre 24 ou 56.
- Un élément d'ordre 14 devrait contenir un 7-cycle et un 2-cycle dans sa décomposition en cycles disjoints, ce qui est impossible dans $\mathfrak{A}_8$. Il n'y a donc pas d'élément d'ordre 14 ou 28.



2-Sylow

Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84

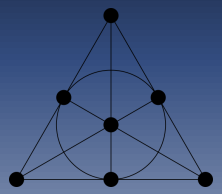
- On sait qu'ils ne peuvent pas être d'ordre 6, ni a fortiori d'ordre 12, 42 ou 84.
- Un élément d'ordre 8 serait un 8-cycle, qui est une permutation impaire. Il n'y a donc ni élément d'ordre 8, ni d'ordre 24 ou 56.
- Un élément d'ordre 14 devrait contenir un 7-cycle et un 2-cycle dans sa décomposition en cycles disjoints, ce qui est impossible dans $\mathfrak{A}_8$. Il n'y a donc pas d'élément d'ordre 14 ou 28.
- On pose $R = \mathcal{O}_2 \cup \mathcal{O}_4$, $R \cup \{1_G\} = \bigcup_{H \in \mathcal{S}_2} H$. $|R| = 63$.



2-Sylow

Un élément d'ordre impair dans G est d'ordre 1, 3, ou 7. Un élément d'ordre pair peut a priori être d'ordre 2, 4, 6, 8, 12, 14, 24, 28, 42, 56 ou 84

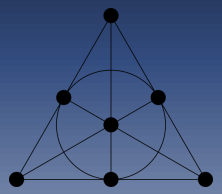
- On sait qu'ils ne peuvent pas être d'ordre 6, ni a fortiori d'ordre 12, 42 ou 84.
- Un élément d'ordre 8 serait un 8-cycle, qui est une permutation impaire. Il n'y a donc ni élément d'ordre 8, ni d'ordre 24 ou 56.
- Un élément d'ordre 14 devrait contenir un 7-cycle et un 2-cycle dans sa décomposition en cycles disjoints, ce qui est impossible dans $\mathfrak{A}_8$. Il n'y a donc pas d'élément d'ordre 14 ou 28.
- On pose $R = \mathcal{O}_2 \cup \mathcal{O}_4$, $R \cup \{1_G\} = \bigcup_{H \in \mathcal{S}_2} H$. $|R| = 63$.
- $63 \leqslant 7|\mathcal{S}_2|$, donc $|\mathcal{S}_2| \geqslant 9$, ce qui laisse comme seule possibilité $|\mathcal{S}_2| = 21$.



2-Sylow

Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

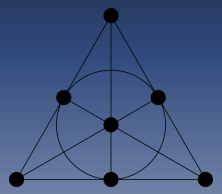
- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.



2-Sylow

Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

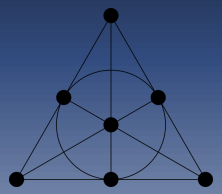
- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.
- Si les 2-Sylow sont abéliens, alors en prenant H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, dont on sait qu'ils existent car sinon G contiendrait au moins $21 \cdot 7$ éléments d'ordre pair, $H \cup H' \subset \mathcal{Z}_v$ avec $|H \cup H'| > 8$.



2-Sylow

Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

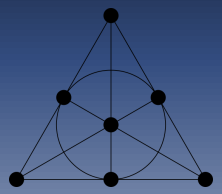
- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.
- Si les 2-Sylow sont abéliens, alors en prenant H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, dont on sait qu'ils existent car sinon G contiendrait au moins $21 \cdot 7$ éléments d'ordre pair, $H \cup H' \subset \mathcal{Z}_v$ avec $|H \cup H'| > 8$.
- Les 2-Sylow sont soit diédraux soit quaternioniques, dans les deux cas, $|\mathcal{O}_4| \neq 0$.



2-Sylow

Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

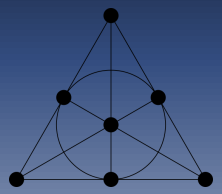
- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.
- Si les 2-Sylow sont abéliens, alors en prenant H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, dont on sait qu'ils existent car sinon G contiendrait au moins $21 \cdot 7$ éléments d'ordre pair, $H \cup H' \subset \mathcal{Z}_v$ avec $|H \cup H'| > 8$.
- Les 2-Sylow sont soit diédraux soit quaternioniques, dans les deux cas, $|\mathcal{O}_4| \neq 0$.
- En étudiant les classes de conjugaison des éléments d'ordre 2 et 4, on trouve $|\mathcal{O}_4| = 42$ et $|\mathcal{O}_2| = 21$, et que tous les éléments d'ordre 2 sont conjugués dans G.



2-Sylow

Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

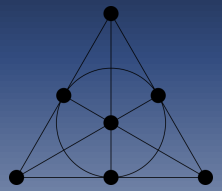
- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.
- Si les 2-Sylow sont abéliens, alors en prenant H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, dont on sait qu'ils existent car sinon G contiendrait au moins $21 \cdot 7$ éléments d'ordre pair, $H \cup H' \subset \mathcal{Z}_v$ avec $|H \cup H'| > 8$.
- Les 2-Sylow sont soit diédraux soit quaternioniques, dans les deux cas, $|\mathcal{O}_4| \neq 0$.
- En étudiant les classes de conjugaison des éléments d'ordre 2 et 4, on trouve $|\mathcal{O}_4| = 42$ et $|\mathcal{O}_2| = 21$, et que tous les éléments d'ordre 2 sont conjugués dans G.
- $\mathcal{Z}_u$ est alors d'ordre 8, c'est un 2-Sylow. Si les 2-Sylow étaient quaternionique, alors pour u d'ordre 2, il y aurait 6 éléments d'ordre 4 dans $\mathcal{Z}_u$, ce qui donnerait $|\mathcal{O}_4| \geqslant 6 \cdot |\mathcal{O}_2| = 126$, ce qui est faux. Les 2-Sylow sont diédraux.



2-Sylow

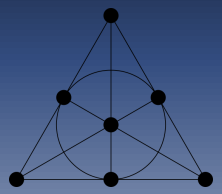
Soit u un élément d'ordre 2. On notera $\mathcal{Z}_u$ le centralisateur de u dans G.

- $\mathcal{Z}_u$ ne contient pas d'élément d'ordre impair, son cardinal est 2, 4 ou 8.
- Si les 2-Sylow sont abéliens, alors en prenant H et H' deux 2-Sylow distincts tels que $H \cap H' \neq \{1_G\}$, dont on sait qu'ils existent car sinon G contiendrait au moins $21 \cdot 7$ éléments d'ordre pair, $H \cup H' \subset \mathcal{Z}_v$ avec $|H \cup H'| > 8$.
- Les 2-Sylow sont soit diédraux soit quaternioniques, dans les deux cas, $|\mathcal{O}_4| \neq 0$.
- En étudiant les classes de conjugaison des éléments d'ordre 2 et 4, on trouve $|\mathcal{O}_4| = 42$ et $|\mathcal{O}_2| = 21$, et que tous les éléments d'ordre 2 sont conjugués dans G.
- $\mathcal{Z}_u$ est alors d'ordre 8, c'est un 2-Sylow. Si les 2-Sylow étaient quaternionique, alors pour u d'ordre 2, il y aurait 6 éléments d'ordre 4 dans $\mathcal{Z}_u$, ce qui donnerait $|\mathcal{O}_4| \geqslant 6 \cdot |\mathcal{O}_2| = 126$, ce qui est faux. Les 2-Sylow sont diédraux.
- Enfin, pour H un 2-Sylow, $\mathcal{N}_G(H) = H$.



Sous-groupes de Klein

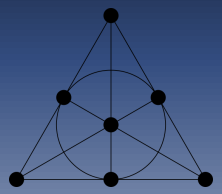
Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.



Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

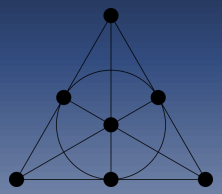
- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.



Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

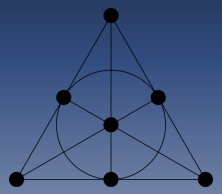
- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.
- $C(\mathcal{Z}_u) = \{1_G, u\}$, donc si $u \neq v$ alors $\mathcal{Z}_u \neq \mathcal{Z}_v$; H est inclus dans 3 2-Sylow disntincts.



Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

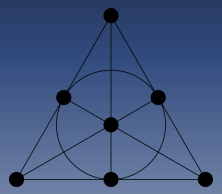
- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.
- $C(\mathcal{Z}_u) = \{1_G, u\}$, donc si $u \neq v$ alors $\mathcal{Z}_u \neq \mathcal{Z}_v$; H est inclus dans 3 2-Sylow disntincts.
- Soit Γ un 2-Sylow, il contient exactement deux groupes de Klein distincts.



Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.
- $C(\mathcal{Z}_u) = \{1_G, u\}$, donc si $u \neq v$ alors $\mathcal{Z}_u \neq \mathcal{Z}_v$; H est inclus dans 3 2-Sylow disntincts.
- Soit Γ un 2-Sylow, il contient exactement deux groupes de Klein distincts.
- Enfin, si $H \subset \Gamma$, alors $u \in C(\Gamma) \backslash \{1_G\}$ est élément de H, c'est-à-dire $\Gamma = \mathcal{Z}_u$, H est contenu dans exactement 3 2-Sylow.

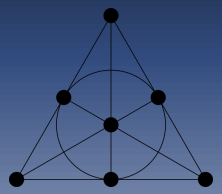


Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.
- $C(\mathcal{Z}_u) = \{1_G, u\}$, donc si $u \neq v$ alors $\mathcal{Z}_u \neq \mathcal{Z}_v$; H est inclus dans 3 2-Sylow disntincts.
- Soit Γ un 2-Sylow, il contient exactement deux groupes de Klein distincts.
- Enfin, si $H \subset \Gamma$, alors $u \in C(\Gamma) \backslash \{1_G\}$ est élément de H, c'est-à-dire $\Gamma = \mathcal{Z}_u$, H est contenu dans exactement 3 2-Sylow.

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



Sous-groupes de Klein

Soit $\mathcal{K}$ l'ensemble des sous-groupes de Klein de G.

- $H \in \mathcal{K}$, et $u \in H \backslash \{1_G\}$; alors $H \subset \mathcal{Z}_u$ qui est un 2-Sylow.
- $C(\mathcal{Z}_u) = \{1_G, u\}$, donc si $u \neq v$ alors $\mathcal{Z}_u \neq \mathcal{Z}_v$; H est inclus dans 3 2-Sylow disntincts.
- Soit Γ un 2-Sylow, il contient exactement deux groupes de Klein distincts.
- Enfin, si $H \subset \Gamma$, alors $u \in C(\Gamma) \backslash \{1_G\}$ est élément de H, c'est-à-dire $\Gamma = \mathcal{Z}_u$, H est contenu dans exactement 3 2-Sylow.

On alors $3 \cdot |\mathcal{K}| = 2 \cdot |\mathcal{S}_2| = 42$, donc $|\mathcal{K}| = 14$.
Étudions $\mathcal{N}_G(H)$: il contient $\mathcal{Z}_u$ pour $u \in H \backslash \{1_G\}$, donc au moins 16 éléments. Un tel u a 21 conjugués dans G, Ainsi, il y a au moins 7 conjugués de H distincts, donc $|\mathcal{N}_G(H)| \leqslant 24$. Comme $|\mathcal{N}_G(H)|$ est un multiple de 4 qui divise 168, c'est 24, et il y a exactement 7 conjugués de H.