propriété.

Par exemple dans $\mathfrak{S}_3$ les trois sous-groupes à 2 éléments $\{1, \tau_a\}$, $\{1, \tau_b\}$ & $\{1, \tau_c\}$ sont conjugués et sont leurs propres normalisateurs.

## 5 – Les théorèmes de Sylow

Thm Lagrange : $G$ groupe fini, $H \subseteq G$ sous-groupe $\Rightarrow |H| \mid |G|$

réciproquement $G$ groupe fini, $|G| = n$, existe-t-il pour tout diviseur $d$ de $n$ un (ou plusieurs) sous-groupe d'ordre $d$ ? la réponse est non en général : $|\mathcal{A}_4| = 12$ et $\mathcal{A}_4$ ne contient pas de sous-groupe d'ordre 6. Néanmoins la réponse est oui dans un cas très important, celui des sous-groupes de Sylow.

Dans ce qui suit $p$ désigne un nombre premier.

**Définition** $G$ groupe fini, $|G| = n$

$p$ diviseur premier de $n$

si $n = p^\alpha m$ avec $p \nmid m$, on appelle **p-sous-groupe de Sylow** de $G$ un sous-groupe d'ordre $p^\alpha$.

**Remarque** dire que $H$ est un p-sous-groupe de Sylow de $G$ signifie que

- $H$ est un p-groupe,
- $[G:H]$ est premier avec $p$.

**Exemple**

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ corps fini à $p$ éléments ($p$ premier)

$G = GL(n, \mathbb{F}_p)$ $n \in \mathbb{N}$

$G$ groupe fini d'ordre

$$|G| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$$

(déterminer $|G|$ revient à déterminer le nombre de bases de $\mathbb{F}_p^n$)

i.e. $$|G| = (p^n - 1)\, p\, (p^{n-1} - 1) \dots p^{n-1} (p-1)$$

soit $$|G| = p \times p^2 \times \dots \times p^{n-1} (p^n - 1)(p^{n-1} - 1) \dots (p^2 - 1)(p-1)$$

ou encore $$|G| = \underbrace{p^{1+2+\dots+n-1}}_{p^{\frac{n(n-1)}{2}}} \underbrace{(p^n - 1)(p^{n-1} - 1) \dots (p^2 - 1)(p-1)}_{m \quad (m \nmid p)}$$

L'ensemble des matrices triangulaires supérieures strictes

$$H = \left\{ A = (a_{ij}) \;\middle|\; \begin{cases} a_{ij} = 0 & \text{si } i > j \\ a_{ii} = 1 \end{cases} \right\}$$

est un p-sous-groupe de Sylow de $G$. En effet comme les $a_{ij}$ sont quelconques pour $i < j$ nous avons

$$|H| = \underset{\substack{\uparrow \\ \text{coeff } 2^{\text{ème}} \\ \text{colonne}}}{p} \times \underset{\substack{\uparrow \\ \text{coeff } 3^{\text{ème}} \\ \text{colonne}}}{p^2} \times \dots \times \underset{\substack{\uparrow \\ \text{coeff nième} \\ \text{colonne}}}{p^{n-1}} = p^{n(n-1)/2}$$

L'énoncé suivant atteste l'existence des sous-groupes de Sylow :

## Théorème (Théorème de Sylow)

G groupe fini

p diviseur (premier) de $|G|$

$\Rightarrow$ G contient au moins un p-sous-groupe de Sylow.

Pour montrer cet énoncé nous avons besoin du lemme suivant qui permet, connaissant un Sylow d'un groupe G, d'en trouver un pour un sous-groupe H :

## Lemme

G groupe avec $|G| = n = p^\alpha m$ avec $p \nmid m$

$H \subseteq G$

S p-Sylow de G

$\exists\, a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H

## Démonstration

Le groupe $G$ opère sur $G/S$ par translation à gauche :

$$G \times G/S \to G/S$$

$$(g, aH) \mapsto g\cdot(aH) = (ga)H$$

Le stabilisateur de $aS$ est

$$\{g \in G \mid g\cdot aS = aS\} = \{g \in G \mid gaS = aS\}$$

$$= \{g \in G \mid g \in aSa^{-1}\}$$

$$= aSa^{-1}$$

Par restriction $H$ opère lui aussi sur $G/S$ avec comme stabilisateur $aSa^{-1} \cap H$.

Montrons que l'un de ces groupes est un Sylow de $H$. Ce sont des $p$-groupes ; il suffit donc que pour un $a \in G$

$\left| H/(aSa^{-1} \cap H) \right|$ soit premier à $p$.

Mais comme nous l'avons vu l'application

$$\begin{aligned} H/_{aSa^{-1}\cap H} &\longrightarrow \mathcal{O}_{aS} \\ \bar{g} &\longmapsto g.aS \end{aligned}$$

est bien définie & est une bijection ; en particulier

$$\left| H/_{aSa^{-1}\cap H} \right| = |\underbrace{\mathcal{O}_{aS}}_{}|$$

orbite de aS dans $G/_S$ sous l'action de H

Si $\left| H/_{aSa^{-1}\cap H} \right|$ était, pour tout $a \in G$, divisible par p, alors il en serait de même pour $|G/_S|$ car $G/_S$ est réunion des orbites $\mathcal{O}_{aS}$ : contradiction avec le fait que S est un p-Sylow de G. ∎

## Démonstration du Théorème

Soit G un groupe et p un diviseur de $|G| = n$. Le théorème de Cayley assure qu'on peut plonger G dans $\mathfrak{S}_n$. Puis on plonge $\mathfrak{S}_n$ dans $GL(n, \mathbb{F}_p)$ de la manière classique à savoir que $\sigma \in \mathfrak{S}_n$ s'envoie sur l'endomorphisme $u_\sigma$ défini dans la base canonique par

$$u_\sigma(e_i) = e_{\sigma(i)}$$

Finalement : on a réalisé $G$ comme un sous-groupe de $GL(n, \mathbb{F}_p)$ qui possède un $p$-Sylow $\underset{\text{Lemme}}{\Longrightarrow}$ $G$ aussi contient un $p$-Sylow. ■

Le deuxième théorème de Sylow étudie la conjugaison des $p$-sous-groupes de Sylow :

**Théorème (Sylow)**

$G$ groupe, $|G| = n = p^\alpha m$ avec $p \nmid m$, $n_p = \#$ $p$-Sylow de $G$

1) $H$ $p$-Sylow de $G$, $K$ $p$-sous-groupe de $G$ $\Rightarrow$ $K$ est contenu dans un conjugué de $H$ : $\exists\, g \in G$ tq $K \subset gHg^{-1}$

2) Les $p$-Sylow sont tous conjugués (et donc $n_p$ divise $n$)

3) On a $n_p \equiv 1 \mod p$ (donc $n_p$ divise $m$)

**Remarque** L'assertion $n_p | n$ résulte du fait que les p-Sylow forment une orbite sous G (on rappelle que l'application

$$\text{ens des classes à gauche } \left\{ \begin{array}{ccc} G/H_x & \longrightarrow & \theta_x \\ \bar{g} & \mapsto & g.x \end{array} \right.$$

est bien définie & est une bijection $\Rightarrow$ lorsque G est fini on a $\frac{|G|}{|H_x|} = |\theta_x|$, en particulier $|\theta_x|$ divise $|G|$).

**Remarque** G groupe fini, $\varphi \in Aut(G)$

S p-Sylow de G $\Rightarrow |\varphi(S)| = |S| = p^\alpha \Rightarrow \varphi(S)$ p-Sylow de G. Si de plus S est l'unique p-Sylow de G, alors $\varphi(S) = S$ : S est un sous-groupe caractéristique de G.

**Corollaire** S p-Sylow de G

$S \triangleleft G \Leftrightarrow$ S est l'unique p-Sylow de G $\Leftrightarrow n_p = 1$

**Rappel** Soit $G$ un $p$-groupe opérant sur un ensemble $X$. Soit

$$X^G = \{ x \in X \mid \forall g \in G \quad g.x = x \}$$

l'ensemble des points fixes sous $G$. Alors $|X| \equiv |X^G| \bmod p$.

## Démonstration du Théorème

$H$ $p$-sous-groupe de $G$

$S$ $p$-Sylow de $G$

$\underset{\text{Lemme}}{\Rightarrow}$ $\exists\, a \in G$ tq $aSa^{-1} \cap H$ $p$-Sylow de $H$

$H$ $p$-groupe $\Rightarrow aSa^{-1} \cap H = H \Rightarrow H \subset \underbrace{aSa^{-1}}_{p\text{-Sylow de } G}$

Si de plus $H$ $p$-Sylow alors $H = aSa^{-1}$.

D'où les deux premières assertions.

Montrons maintenant la troisième assertion. Faisons opérer $G$ par conjugaison sur l'ensemble $X$ de ses $p$-Sylow :

$$\begin{aligned} G \times X &\to X \\ (g, H) &\mapsto g.H = gHg^{-1} \end{aligned}$$

Soit $S$ un $p$-Sylow ; $S$ opère sur $X$ et on a

$$|X| \equiv |X^S| \mod p$$

Montrons que $|X^S| = 1$ :

si $s \in S$ alors $sSs^{-1} = S$ : $S \in X^S \Rightarrow$ montrer que $|X^S| = 1$ revient à montrer que $S$ est l'unique élément de $X^S$.

Soit $T \in X^S$, $T$ est un $p$-Sylow tq

$$\forall s \in S \qquad sTs^{-1} = T \quad (*)$$

Soit $N = \langle T, S \rangle \subseteq G$. On a $S \subset N$
$T \subset N$
$S$ & $T$ sont des $p$-Sylow de $N$

$S$ normalise $T$ $(*)$ $\Rightarrow T \triangleleft N$

Corollaire $\Rightarrow T$ unique Sylow de $N \Rightarrow S = T$

Les $p$-Sylow forment une orbite sous $G \Rightarrow n_p \mid |G| = p^\alpha m$

mais $n_p \equiv 1 \mod p \Rightarrow n_p \mid m$. ■

## Corollaire (Théorème de Cauchy)

$G$ groupe

$p$ nombre premier divisant $|G|$

$\Rightarrow$ $G$ contient un élément d'ordre $p$

## Démonstration

Ecrivons $|G|$ sous la forme $p^\alpha m$ où $\alpha \geq 1$ et $m$ est premier avec $p$.

Raisonnons par l'absurde : supposons qu'aucun élément de $G$ soit d'ordre $p$. Alors l'ordre de tout élément de $G$ n'est pas divisible par $p$ ; en effet si $|\langle g \rangle| = ap$, alors $g^a$ est d'ordre $p$.

En particulier tout élément du $p$-Sylow de $G$ (l'existence de ce $p$-Sylow est assurée par le premier théorème de Sylow) est d'ordre non divisible par $p$ et par ailleurs cet ordre divise $p^a$ : contradiction. ■

## Corollaire

$G$ groupe tel que $|G| = p^\alpha m$ avec $p \nmid m$

$\Rightarrow$ $G$ contient des sous-groupes d'ordre $p^i$ $\forall i \leq \alpha$

## Démonstration

$S$ $p$-Sylow de $G$ $\Rightarrow$ $|S| = p^\alpha$

$S$ $p$-Sylow de $G$ $\Rightarrow$ $S$ $p$-groupe de $G$ $\Rightarrow$ $Z(S) \neq \{1\}$

Théorème de Cauchy $\Rightarrow$ $Z(S)$ contient un élément $g$ d'ordre $p$

- $\langle g \rangle$ est un sous-groupe de $S \subset G$ d'ordre $p$ : nous avons montré l'énoncé pour $i = 1$
- supposons que pour tout sous-groupe de $S$ d'ordre $p^i$, $i < \alpha$, contient un sous-groupe d'ordre $p^j$ pour tout entier $j \leq i$.

Hypothèse de récurrence $\Rightarrow$ il existe un sous-groupe $H_{i-1}$ d'ordre $p^{i-1}$ dans $S/\langle g\rangle$.

$\pi : S \to S/\langle g\rangle$ projection canonique

$\pi^{-1}(H_{i-1}) \leq S \Rightarrow \pi^{-1}(H_{i-1}) \leq G$ & $|\pi^{-1}(H_{i-1})| = p^i$. ∎

## Exemple : le cas $GL(n, \mathbb{F}_p)$

$p$ premier. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ = corps fini à $p$ éléments

$G = GL(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$

déjà vu : l'ensemble des matrices triangulaires supérieures

$$P = \left\{ A = (a_{ij}) \;\middle|\; \begin{cases} a_{ij} = 0 \text{ si } i > j \\ a_{ii} = 1 \end{cases} \right\}$$

est un $p$-Sylow de $G$

2ème théorème de Sylow $\Rightarrow$ les $p$-Sylow de $G$ sont de la forme

$MPM^{-1}$ où $M \in GL(n, \mathbb{F}_p)$

## Exemple : un groupe d'ordre 63 n'est pas simple

$G$ groupe d'ordre 63

rem : $63 = 3^2 \times 7$ => on s'intéresse aux sous-groupes de Sylow d'ordre 7

3ème thm Sylow

$$\left.\begin{array}{l} \text{d'une part } n_7 \equiv 1 \text{ mod } 7 \\ \text{d'autre part } n_7 \mid 9 \end{array}\right\} \Rightarrow n_7 = 1$$

i.e. $G$ contient un seul 7 - Sylow qui est donc (Corollaire) distingué dans $G$ : $G$ n'est pas simple.

## Exemple : les groupes $\mathfrak{S}_4$ & $\mathcal{A}_4$

$\nu_p = \#$ p- Sylow de $\mathfrak{S}_4$

$n_p = \#$ p - Sylow de $\mathcal{A}_4$

$|\mathfrak{S}_4| = 2^3 \times 3$ & $|\mathcal{A}_4| = 2^2 \times 3$ => on s'intéresse aux 2- Sylow & aux 3- Sylow

3ème thm de Sylow $\Rightarrow \begin{cases} \nu_3 \mid 2^3 = 8 & \& \ \nu_3 \equiv 1 \mod 3 \\ \nu_2 \mid 3 & \& \ \nu_2 \equiv 1 \mod 2 \\ n_3 \mid 2^2 = 4 & \& \ n_3 \equiv 1 \mod 3 \\ n_2 \mid 3 & \& \ n_2 \equiv 1 \mod 2 \end{cases}$

$\Rightarrow \quad \nu_3 \in \{1, 4\}, \quad \nu_2 \in \{1, 3\}, \quad n_3 \in \{1, 4\}, \quad n_2 \in \{1, 3\}$

• 3-Sylow de $\mathfrak{S}_4$ & $\mathcal{A}_4$

un 3-Sylow de $\mathfrak{S}_4$ = sous-groupe de $\mathfrak{S}_4$ d'ordre 3 i.e. isomorphe à $\mathbb{Z}/3\mathbb{Z}$ ou encore un sous-groupe engendré par un élément d'ordre 3

les seuls éléments d'ordre 3 de $\mathfrak{S}_4$ sont les 3-cycles $\Rightarrow$ les 3-Sylow de $\mathfrak{S}_4$ sont $\{id, (1\ 2\ 3), (1\ 3\ 2)\}$, $\{id, (1\ 2\ 4), (1\ 4\ 2)\}$, $\{id, (1\ 3\ 4), (1\ 4\ 3)\}$, $\{id, (2\ 3\ 4), (2\ 4\ 3)\}$

$\Rightarrow \nu_3 = 4$

<u>rem</u> : tous ces groupes sont contenus dans $\mathcal{A}_4$ $\Rightarrow$ tous ces groupes sont les 3-Sylow de $\mathcal{A}_4$ $\Rightarrow n_3 = 4$

## • 2-Sylow de $\mathcal{S}_4$

$E$ = partitions de $\{1,2,3,4\}$ en deux sous-ensembles à deux éléments $\Rightarrow E = \{P_1, P_2, P_3\}$ où

$P_1 = \{1,2\} \sqcup \{3,4\}$ $\quad P_2 = \{1,3\} \sqcup \{2,4\}$ $\quad P_3 = \{1,4\} \sqcup \{2,3\}$

Considérons l'action de $\mathcal{S}_4$ sur $E$ :

$(2\ 3) . P_1 = P_2$ $\qquad (2\ 4) . P_1 = P_3$

$\Rightarrow$ l'action est transitive $\Rightarrow |\mathrm{Stab}_{\mathcal{S}_4}(P_1)| = \dfrac{|\mathcal{S}_4|}{|\mathcal{O}_{P_1}|} = \dfrac{24}{3} = 8$

$\Rightarrow \mathrm{Stab}_{\mathcal{S}_4}(P_1)$ est un 2-Sylow de $\mathcal{S}_4$

$\Rightarrow \{$2-Sylow de $\mathcal{S}_4\} = \{$conjugués de $\mathrm{Stab}_{\mathcal{S}_4}(P_1)\}$

$\Rightarrow \{$2-Sylow de $\mathcal{S}_4\} = \{\mathrm{Stab}_{\mathcal{S}_4}(P_1), \mathrm{Stab}_{\mathcal{S}_4}(P_2), \mathrm{Stab}_{\mathcal{S}_4}(P_3)\}$

$\uparrow$

$G$ groupe opérant sur $E$, si $x \in E$, si $y \in Gx$, alors

$\mathrm{Stab}_G(y)$ est égal au conjugué de $\mathrm{Stab}_G(x)$ par n'importe quel élément de $G$ qui envoie $x$ sur $y$). Or

2- Sylow de $\mathfrak{S}_4$

$$\mathrm{Stab}_{\mathfrak{S}_4}(P_1) = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 2), (3\ 4)\}$$

$$\mathrm{Stab}_{\mathfrak{S}_4}(P_2) = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4)\}$$

$$\mathrm{Stab}_{\mathfrak{S}_4}(P_3) = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4), (2\ 3)\}$$

ils sont 2 à 2 distincts $\Rightarrow \nu_2 = 3$

- 2- Sylow de $\mathfrak{A}_4$

$$\mathrm{Stab}_{\mathfrak{S}_4}(P_1) \cap \mathrm{Stab}_{\mathfrak{S}_4}(P_2) \cap \mathrm{Stab}_{\mathfrak{S}_4}(P_3)$$

$$= \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

cette intersection coïncide avec le noyau du morphisme

$\mathfrak{S}_4 \to \mathfrak{S}_E \simeq \mathfrak{S}_3$ induit par l'action de $\mathfrak{S}_4$ sur $E$ $\Rightarrow$ c'est un sous-groupe distingué de $\mathfrak{S}_4$ contenu dans $\mathfrak{A}_4$ $\Rightarrow$ est a fortiori distingué dans $\mathfrak{A}_4$ $\Rightarrow$ c'est le seul 2-Sylow de $\mathfrak{A}_4$.

Corollaire

Remarque retour sur les $\mathrm{Stab}_{\mathfrak{S}_4}(P_i)$ ; détaillons le cas $\mathrm{Stab}_{\mathfrak{S}_4}(P_1)$ :

$$\begin{aligned}
\mathrm{Stab}_{\mathfrak{S}_4}(P_1) &= \{\sigma \in \mathfrak{S}_4 \mid \sigma(P_1) = P_1\} \\
&= \{\sigma \in \mathfrak{S}_4 \mid \sigma(\{1,2\}) = \{1,2\} \ \& \ \sigma(\{3,4\}) = \{3,4\}\} \\
&\quad \cup \{\sigma \in \mathfrak{S}_4 \mid \sigma(\{1,2\}) = \{3,4\} \ \& \ \sigma(\{3,4\}) = \{1,2\}\} \\
&= \{id, (1\ 2)(3\ 4), (1\ 2), (3\ 4)\} \\
&\quad \cup \{id, (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 4)(2\ 3)\}
\end{aligned}$$