Théorèmes de Sylow

[PERRIN]

1. Soit G groupe fini, p un diviseur premier de $|G|$. Alors G contient au moins un p-ssgpe de Sylow.

Pour démontrer ça, on va utiliser 2 lemmes.

<u>Lemme 1</u> $|G| = n = p^\alpha m$, $p \nmid m$, H ssgpe de G, S p-Sylow de G. Alors $\exists a \in G$, $aSa^{-1} \cap H$ est un p-Sylow de H.

G opère sur G/S par translation à gche, donc par restriction H agit aussi de la m̂ façon sur G/S.

$$\begin{aligned}\forall a \in G, \quad \mathrm{Stab}_H(aS) &= \{h \in H / h.aS = aS\} \\ &= \{h \in H / a^{-1}haS = S\} \\ &= \{h \in H / a^{-1}ha \in S\} \\ &= aSa^{-1} \cap H.\end{aligned}$$

Reste à mq l'un de ces gpes est un p-Sylow de H.
- ▸ $aSa^{-1} \cap H$ p-gpe en tant que ssgpe du p-Sylow aSa^{-1}
- ▸ Mq $\exists a \in G$, $|H/(aSa^{-1} \cap H)| \wedge p = 1$.

<u>Eq aux classes</u> : $$|G/S| = \sum_{aS \in \Omega} \frac{|H|}{|aSa^{-1} \cap H|}$$

avec Ω partie de G/S constituée exactement d'un représentant de chaque orbite.

$p \nmid |G/S|$ car S p-Sylow de G donc $[G:S] \wedge p = 1$

Par hypothèse, dc $\exists aS \in \Omega$ tq $p \nmid \left|\frac{H}{aSa^{-1} \cap H}\right|$ dc $p \wedge [H : aSa^{-1} \cap H] = 1$

dc fft, d'après ces 2 pts, on a : $\exists a \in G$, $aSa^{-1} \cap H$ p-Sylow de H. ■

<u>Lemme 2</u> Soit $n \in \mathbb{N}^*$. Alors $GL_n(\mathbb{F}_p)$ possède un p-Sylow.

on a : $$|GL_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1} (p^n - p^i) = (pp^2 \cdots p^{n-1})\, m, \quad m \wedge p = 1$$
$$= p^{\frac{(n-1)n}{2}}\, m.$$

on exhibe un p-Sylow de $GL_n(\mathbb{F}_p)$:
$$H = \{A = (a_{ij}) \;/\; a_{ij} = 0,\ i > j \text{ et } a_{ii} = 1\}$$
$$|H| = pp^2 \cdots p^{n-1} = p^{n(n-1)/2}$$ ■

<u>Démo 1.</u> Soit G gpe, p diviseur de $n = |G|$

On plonge G dans $\mathfrak{S}_n$ par thm de Cayley (ie $\exists$ une injection entre G et $\mathfrak{S}_n$)

On plonge $\mathfrak{S}_n$ ds $GL_n(\mathbb{F}_p)$ avec l'appli inj $\begin{array}{l}\mathfrak{S}_n \longrightarrow GL_n(\mathbb{F}_p) \\ \sigma \longmapsto P_\sigma\end{array}$

avec P_σ matrice de permutation.

On a donc $G \simeq$ ssgp $GL_n(\mathbb{F}_p)$ qui possède un p-sylow par lemme 2 donc par lemme 1, G possède un p-Sylow. ■

---

2. Si H p-ssgpe de G, $\exists S$ p-Sylow tq $H \subset S$

3. Les p-Sylow sont tous conjugués

- si H p-ssgpe et S p-Sylow de G, alors par lemme 1, $\exists a \in G$, $aSa^{-1} \cap H$ est un p-Sylow de H et $aSa^{-1} \cap H \overset{\text{car } H \text{ p-gpe}}{=} H$.
  donc $H \subset aSa^{-1}$ qui est un p-Sylow (on a montré 2.)
- De plus, si H p-Sylow, on a $H = aSa^{-1}$ car $H \subset aSa^{-1}$ et $o(H) = p^\alpha = o(aSa^{-1})$. ■

---

4. $n_p \equiv 1\ [p]$ et $n_p \mid m$

- Soit X l'ens des p-Sylow de G ($n_p = |X|$).

On fait opérer G par conjugaison sur X :
$$\begin{array}{l} G \times X \longrightarrow X \\ (g, H) \longmapsto gHg^{-1} \end{array}$$

Soit S p-Sylow de G. Par restriction, S opère aussi sur X par conjugaison.

On note $X^S = \{H \in X / \forall s \in S,\ s.H = H\}$.

Alors $|X| \equiv |X^S|\ [p]$ ie $n_p \equiv |X^S|\ [p]$.

Mq $|X^S| = 1$.

- * $S \in X^S$ donc $|X^S| \geq 1$
- * Soit $T \in X^S$. Soit $N = \langle S, T \rangle$ ssgpe de G engendré par S et T.

On a $S \subset N$ et $T \subset N$ et ce sont des p-Sylow de N.
et $T \in X^S$ donc $\forall s \in S \subset N$, $sTs^{-1} = T$ donc $T \triangleleft N$.

Ainsi T est l'unique p-Sylow de N.
(en effet, supp $\exists U$ autre p-Sylow de N. Alors U et T sont conjugués
donc $\exists a \in N$, $aTa^{-1} = U$.
or $T \triangleleft N$ donc $\forall m \in N$, $mTm^{-1} = T$.
donc en particulier pour $a = m$
donc $T = aTa^{-1} = U$.)
or S p-Sylow de N dc $T = S$ par unicité.
donc $|X^S| = 1$
$\Rightarrow m_p \equiv 1 [p]$.

• Mq $m_p | m$
Soit S p-Sylow de G.
$m = |G| = |Stab(S)| \times |Orb(S)|$ pour l'action de conjug. de G sur X.
or $|Orb(S)| = m_p$ car ts les p-ssgpes de Sylow sont conjugués
d'où $m_p | m = p^\alpha m$.
or $m_p \equiv 1 [p] \Rightarrow p \wedge m_p = 1$
donc $m_p | m$. ∎

• Th de Cayley : Tout gpe G est isomorphe à un ssgpe de $\mathfrak{S}_m$.
dc $\exists \varphi : G \longrightarrow$ ssgpe de $\mathfrak{S}_m$ isomorph (dc injection).
on mq l'action de G sur G par translation est fidèle.

Rques : • La restriction $H \hookrightarrow G/S$ est bien déf car H ssgpe de G
⚠ Soit $G \hookrightarrow X$ action, Y ss ens de X. $G \hookrightarrow Y$ est déf ssi Y orbites ou réunion d'orbites (ex : $\mathfrak{S}_m \hookrightarrow \{1, \dots, m\}$ ok mais $\mathfrak{S}_m \hookrightarrow \{1\}$ pas déf)
• S p-Sylow de G ssi $[G:S] \wedge p = 1$ et S p-gpe
• $|GL_m(\mathbb{F}_p)| = \prod_{k=0}^{m-1} (p^m - p^k)$
* $e_1 \neq 0 \rightarrow$ p choix par coord du vecteur de $p^m - 1$ possibilités
* e_2 tq (e_1, e_2) libre $\rightarrow p^m - p$ possibi ...
• $A = \begin{pmatrix} 1 & a_{21} & \cdots & a_{m1} \\ & \ddots & & \vdots \\ (0) & & \ddots & a_{m-1,m} \\ & & & 1 \end{pmatrix} \in GL_m(\mathbb{F}_p)$
* C_1 : 0 coeff $\rightarrow$ 0 choix
C_2 : 1 coeff $\rightarrow$ p choix
C_3 : 2 coeff $\rightarrow$ p^2 choix
⋮
et $\prod_{k=0}^{m-1} p^k = p^{\sum_{k=0}^{m-1} k} = p^{m(m-1)/2}$

• $X^G = \{x \in X / \forall g \in G, g.x = x\}$. Mq $|X| \equiv |X^G| [p]$
$x \in X^G \iff \forall g \in G, g.x = x \iff G.x = \{x\}$
$\left(\text{or } \bigsqcup_{x \in X} G.x = X \right)$
si $x \notin X^G$, $|G.x| > 1$ et comme $|G.x| \mid o(G) = p^\alpha$, $p \mid |G.x|$
et $|X| = \sum_{x \in X^G} |G.x| + \sum_{x \notin X^G} |G.x|$
$\equiv |X^G| [p]$

• $N = \langle S, T \rangle$. Pq S, T p-Sylow de N ? $o(G) = p^\alpha m$
N ssgpe de G donc $o(N) = p^\lambda m'$, $\lambda < \alpha$, $m' | m$
et S, T p-Sylow de G dc d'ordre p^α et $S, T \subset N$ donc la puissance α est maximale dans N.
• $|Orb(S)| = \{gSg^{-1} / g \in G\}$ et p-Sylow ts conju dc $|Orb S| = m_p$

• Pq $o(G) = |Stab(S)| \times |Orb(S)|$?
on a une bijection entre G/G_x et $G.x$ ie ici entre $G/Stab(S)$ et $Orb(S)$
donc $\dfrac{o(G)}{|Stab(S)|} = |Orb(S)|$