Théorèmes de Sylow

Soit p un nombre premier.

75.1 **Déf** G est un p-groupe $\Leftrightarrow$ $\begin{cases} G \text{ est un groupe fini.} \\ \text{il existe } n \in \mathbb{N} \text{ tel que } \mathrm{Card}(G) = p^n \end{cases}$

Dans toute la suite on considère un groupe fini G tel que $\mathrm{Card}(G) = p^n q$ où $n \in \mathbb{N}^*$ et $p \nmid q$

75.2 **Déf** H est un p-Sylow de G $\Leftrightarrow$ $H < G$ et $\mathrm{Card}(H) = p^n$

Rq • Le conjugué dans G d'un p-Sylow de G reste un p Sylow de G car la conjugaison ne change pas le cardinal.

• p Sylow $\Rightarrow$ p sous-groupe $\Rightarrow$ p groupe.

75.3 **Lemme 1** $\binom{p^n q}{p^n} \equiv q \ [p]$

Preuve Pour $k \in [\![1, p-1]\!]$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!\binom{p}{k}$.

Or $p \mid p!$

$p \nmid k!$ car $p > k$ (donc $\forall i \in [\![1,k]\!]$ $p \nmid i$, donc $p \nmid \prod_{i=1}^{k} i = k!$)

$p \nmid (p-k)!$ car $p > p-k$.

Donc $p \mid \binom{p}{k}$. Donc dans $\mathbb{F}_p$ $\binom{p}{k} = 0$. ($\binom{p}{k} \equiv 0 \ [p]$)

On considère $(1+X)^p$ comme polynôme de $\mathbb{F}_p[X]$.

Dans $\mathbb{F}_p$, corps commutatif, on peut utiliser le binôme de Newton, donc $(1+X)^p = \sum_{k=0}^{p} \binom{p}{k} X^k 1^{p-k}$

$= 1^p + X^p$ (car $\forall k \in [\![1, p-1]\!]$ $\binom{p}{k} = 0$ dans $\mathbb{F}_p$ et $\binom{p}{p} = \binom{p}{0} = 1$)

$= 1 + X^p$

En itérant cet argument on obtient que $(1+X)^{p^n} = 1+X^{p^n}$.
Toujours dans $\mathbb{F}_p[X]$ on considère maintenant $(1+X)^{p^n q}$.
D'une part $(1+X)^{p^n q} = \left((1+X)^{p^n}\right)^q$
$= \left(1+X^{p^n}\right)^q$
$= \sum_{k=0}^{q} \binom{q}{k} \left(X^{p^n}\right)^k 1^{p-k}$ } binôme

D'autre part $(1+X)^{p^n q} = \sum_{k=0}^{p^n q} \binom{p^n q}{k} X^k 1^{p-k}$ (binôme)

En identifiant le coefficient devant X^{p^n} dans les deux expressions on obtient $\binom{p^n q}{p^n} = \binom{q}{1} = q$ (dans $\mathbb{F}_p$)
On en déduit $\binom{p^n q}{p^n} \equiv q \,[p]$

75.4 **Lemme 2** $H < G$, S p-Sylow de G $\Rightarrow \exists g \in G,\ gSg^{-1} \cap H$ est p-Sylow de H

Démonstration * D'après le théorème de Lagrange (q) $|H| \mid |G|$, soit $|H| \mid p^n q$. Il existe donc $n' \leq n$ et $q' \mid q$ tel que $|H| = p^{n'} q'$ (rq $p \nmid q'$ sinon $p \mid q$).

* On note X le quotient $G/S = \{gS \mid g \in G\}$
H agit sur X par translation $(h, gS) \mapsto (hg)S$)
$|X| = |G|/|S| = p^n q / p^n = q$ or $p \nmid q$ donc $p \nmid |X|$
Or par la formule des classes, $|X|$ est la somme des cardinaux des H-orbites de G/S, il existe donc une orbite dont le cardinal n'est pas divisible par p, donc il existe $g \in G$ tq $p \nmid |O_H(gS)|$.
Or $|O_H(gS)| = \dfrac{|H|}{|\mathrm{Stab}_H(gS)|}$ donc $p \nmid \dfrac{|H|}{|\mathrm{Stab}_H(gS)|}$

Montrons de plus que $\mathrm{Stab}_H(gS) = gSg^{-1} \cap H$.

- $\mathrm{Stab}_H(gS) \subset H$ par définition
- Si $h \in \mathrm{Stab}_H(gS)$ $h \cdot gS = gS$ c-à-d $hgS = gS$ donc $(hg)S = gS$,
Il existe donc $s \in S$ tel que $hg = gs$, alors $h = gsg^{-1} \in gSg^{-1}$.

D'où $\mathrm{Stab}_H(gS) \subset gSg^{-1} \cap H$.

Réciproquement si $h \in gSg^{-1} \cap H$, alors il existe $s \in S$ tel que $h = gsg^{-1}$. Alors $h \cdot gS = (hg)S = (gsg^{-1}g)S = gsS = gS$. Donc $h \in \mathrm{Stab}_H(gS)$
Donc $gSg^{-1} \cap H \subset \mathrm{Stab}_H(gS)$

On a donc $p \nmid \frac{|H|}{|H \cap gSg^{-1}|}$

De plus par th. de Lagrange, puisque $H \cap gSg^{-1} < gSg^{-1}$ $|H \cap gSg^{-1}| \mid |gSg^{-1}|$
Or $|gSg^{-1}| = |S| = p^n$ car S est un p Sylow, donc $|H \cap gSg^{-1}| \mid p^n$
donc il existe $m \in \mathbb{N}$ tel que $|H \cap gSg^{-1}| = p^m$ et $m \leq n$.

On réécrit $p \nmid \frac{|H|}{|H \cap gSg^{-1}|}$ en $p \nmid \frac{p^{n'}q'}{p^m}$; donc $m = n'$

et $\mathrm{Card}(gSg^{-1} \cap H) = p^{n'}$, d'où $gSg^{-1} \cap H$ est un p-Sylow de H.

Théorème de Sylow

où G vérifie $\mathrm{Card}(G) = p^n q$.

75.5 · G admet au moins un p-Sylow

75.6 · Deux p-Sylows de G sont néc. conjugués dans G

75.7 · Tout p-sous-groupe de G est contenu dans un p-Sylow.

Preuve a) Construisons un p-Sylow.
On considère $E = \mathcal{P}_{p^n}(G)$ l'ens. des parties à p^n élém^t de G.
C'est dans E qu'on cherche notre p-Sylow (par déf, E les contient tous)
$\mathrm{Card}(E) = \binom{p^n q}{p^n}$.
G agit sur E par $\left(\begin{array}{c} G \times E \to E \\ g \cdot A \mapsto gA = \{ga \mid a \in A\} \end{array}\right)$.
Par la formule des classes $\mathrm{Card}(E)$ est la somme des cardinaux des G-orbites de E.

Or d'après le lemme 1, $p \nmid \binom{p^n q}{p^n} = \mathrm{Card}(E)$.
Donc nécessairement l'une de ces orbites est de cardinal non-divisible par p, autrement dit il existe $A \in E$, tel que $p \nmid |O_G(A)|$
Soit $g \in G$ tel que $g^{-1} \in A$. $Ag \in E$ car $|Ag| = |A| = p^n$.
$O_G(Ag) = \{g' \cdot Ag \mid g' \in G\} = \{g'Ag \mid g' \in G\} = \{g'A \mid g' \in G\}g = \{g' \cdot A \mid g' \in G\}g = O_G(A)g$
Donc $|O_G(Ag)| = |O_G(A)g| = |O_G(A)|$.
Donc $p \nmid |O_G(Ag)|$.

On pose alors $S = Ag$. $|S| = |Ag| = |A| = p^n$. $g^{-1}g \in Ag$ donc $e \in S$
Il reste donc à MQ S est bien un sous-groupe.
On considère $H = \mathrm{Stab}_G(S) = \{h \in G \mid h \cdot S = S\}$
- Si $h \in H$, $h = he = h \underbrace{\cdot}_{H's} S = S$ donc $h \in S$. D'où $H \subset S$

⚠ On peut être tenté de dire que $S \subset H$ car si $s \in S$ $sS = S$.
Or ça ne serait vrai que si on savait déjà que S est 1 ss gpe

- $|O_G(S)| = \frac{|G|}{|\mathrm{Stab}_G(S)|} = \frac{p^m q}{|H|}$. Donc $|H| \mid p^m q$ (Sat $|H| = p^{m'} q'$ où $m' \leq m$ et $q' \mid q$)

or $|O_G(S)| = |O_G(A)|$ donc $p \nmid \frac{p^m q}{|H|}$ donc $p \nmid \frac{p^{m'} q'}{|H|}$
(en effet $p \nmid p^{m-m'} q/q'$ donc $m - m' = 0$ donc $|H| = p^m q'$ soit $p \nmid |H|$)
Donc $|H| \geq p^n = |S|$.
On en déduit $H = S$.
Comme H est un sous groupe de G en tant que Stab_G, S est bien un sous-groupe de G de cardinal p^n, soit un p-Sylow.

b) Soient S et T deux p-Sylow de G.
En voyant T comme sous-groupe de G et S comme p-Sylow, le lemme 2 nous donne l'existence de $g \in G$ tel que $|gSg^{-1} \cap T|$ soit un p-Sylow de T. Puisque $\mathrm{Card}(T) = p^m$, cela implique $|gSg^{-1} \cap T| = p^n$, avec l'inclusion $gSg^{-1} \cap T \subset T$ on en conclut l'égalité $gSg^{-1} = T$. Donc S et T sont bien conjugués.

c) Soit H un p-sous groupe de G. il existe $n' \in \mathbb{N}$ tq $|H| = p^{n'}$.
D'après (a) on sait qu'il existe un p-Sylow S.
D'après le lemme 2, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H ; c-à-d notamment $|gSg^{-1} \cap H| = p^{n'} = |H|$
Or on a l'inclusion $gSg^{-1} \cap H \subset H$, donc $gSg^{-1} \cap H = H$,
soit $H \subset gSg^{-1}$, or gSg^{-1} est bien un p-Sylow.

Théorème de Sylow (bis) où G vérifie $\mathrm{Card}(G) = p^n q$

En notant s_p le nombre de p-Sylow de G on a :

75.8 • $s_p \mid q$

75.9 • $s_p \equiv 1 \ [p]$

Preuve On note E l'ensemble des p-Sylow de G. $s_p = \mathrm{Card}(E)$.

(a). G agit sur E par conjugaison, en effet le conjugué dans G d'un p Sylow reste un p-Sylow de G.
• De plus cette action est transitive, c'est exactement 7.5.6.
Soit $S \in E$. Par transitivité $O_G(S) = E$ donc $s_p = |O_G(S)|$
Or $|O_G(S)| = \dfrac{|G|}{|\mathrm{Stab}_G(S)|} = \dfrac{p^n q}{|\mathrm{Stab}_G(S)|}$

$\left.\begin{array}{l} \mathrm{Stab}_G(S) < G \\ S < G \\ S \subset \mathrm{Stab}_G(S) \text{ car } \forall s \in S,\ sSs^{-1} = S \end{array}\right\}$ donc $S < \mathrm{Stab}_G(S)$.
Par Lagrange $|S| \mid |\mathrm{Stab}_G(S)|$

Soit $p^n \mid |\mathrm{Stab}_G(S)|$ (donc $|\mathrm{Stab}_G(S)| = p^n q'$ et $|O_G(S)| = \dfrac{p^n q}{p^n q'} = \dfrac{q}{q'}$, d'où $q = |O_G(S)| q'$)
donc $|O_G(S)| \mid q$
D'où $s_p \mid q$

(b) Soit $S \in E$. $S \subset G$ donc par restriction de l'action précédente, S agit par conjugaison sur E.
- S, vu comme élément de E, est point fixe pour cette action.

En effet $\forall s \in S$, $sSs^{-1} = S$. Montrons que c'est le seul.
Soit $T \in E$. On le suppose S-fixe, c-à-d $\forall s \in S$ $sTs^{-1} = T$.
Alors $ST < G$ et $|ST| = \frac{|S| \times |T|}{|S \cap T|}$ (f ~~~~)

$S \cap T < S$, donc par Lagrange $|S \cap T| \,|\, |S| = p^n$, donc il existe $m \in \mathbb{N}$ tel que $|S \cap T| = p^m$ où $\underline{m \leq n}$
Donc $|ST| = \frac{p^n \times p^n}{p^m} = p^{2n-m}$.
Or $ST < G$ donc par Lagrange $|ST| \,|\, |G|$
soit $p^{2n-m} \,|\, p^n q$, or puisque $p \nmid q$ cela revient à $p^{2n-m} \,|\, p^n$ donc $2n - m \leq n$ donc $\underline{n \leq m}$
D'où $n = m$ et $|ST| = p^n$ et $|S \cap T| = p^m = |S| = |T|$
Or on a les inclusions évidentes : $S \cap T \subset S$, $S \cap T \subset T$
On en déduit $S \cap T = T$ et $S \cap T = S$ d'où $\underline{S = T}$.

Une S-orbite de E est → soit réduite à un point fixe, donc de card 1
→ soit non réduite à un point et de cardinal
car $|\mathcal{O}_S(x)| = \frac{|S|}{|\mathrm{Stab}_S(x)|}$ ⟶ diviseur de $|S| = p^n$, soit de la forme p^k avec $k \geq 1$

Donc $\mathrm{Card}(E)$, dont on sait par la formule des classes qu'il s'écrit comme somme des cardinaux des orbites, ne fait apparaître que des p^{k_i}, et un 1 pour son seul point fixe.
D'où $\mathrm{Card}(E) \equiv 1 \,[p]$ soit $s_p \equiv 1 \,[p]$