DEV : THÉORÈMES DE SYLOW

Réf : PERRIN, "Cours d'Algèbre" p. 18-19.
RONBALDI, "Math pour l'agreg : Algèbre et Géom" p 155-156.

PRÉLIMINAIRE : On montre que $Gl_n(\mathbb{F}_p)$ pour p premier admet un p-Sylow.

Note $G = Gl_n(\mathbb{F}_p)$. Alors G est un groupe fini de cardinal

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

En effet, il suffit de compter les bases de $(\mathbb{F}_p)^n$. Soit $A \in Gl_n(\mathbb{F}_p)$. Alors les colonnes de A forment une base pour $(\mathbb{F}_p)^n$. Compter les matrices de G revient à compter le nombre de bases de $(\mathbb{F}_p)^n$. Regardons le nombre de façons de choisir une telle base $(e_i)_{1 \le i \le n}$. On commence par choisir e_1 quelconque dans $(\mathbb{F}_p)^n \setminus \{0\}$ On a donc $p^n - 1$ choix. Puis pour k entre 2 et n on suppose $e_1, \dots, e_{k-1}$ choisi linéairement indépdt dans $\mathbb{F}_p{}^n \setminus \{0\}$. On choisi e_k dans $(\mathbb{F}_p)^n \setminus \{0\}$ de manière à ce qu'il soit lin. indép. avec les $e_1, \dots, e_{k-1}$. On le prend donc ds $(\mathbb{F}_p)^n \setminus \bigoplus_{i=1}^{k-1} \mathbb{F}_p e_i$.

On $\operatorname{card}\left((\mathbb{F}_p)^n \setminus \bigoplus_{i=1}^{k-1} \mathbb{F}_p e_i\right) = \operatorname{card}(\mathbb{F}_p{}^n) - \prod_{i=1}^{k-1} \operatorname{card}(\mathbb{F}_p e_i)$

$= p^n - p^{k-1}$

$\left|\bigoplus_{i=1}^{n} F_i\right| = \prod_{i=1}^{n} |F_i|$ car par déf de $\oplus$, $F_1 \times \cdots \times F_n \xrightarrow{\text{bij}} \bigoplus_{i=1}^{n} F_i$, $(x_1, \dots, x_n) \mapsto x_1 + \cdots + x_n$

$|\mathbb{F}_p e_i| = |\mathrm{Vect}_{\mathbb{F}_p}(e_i)| = |\{\lambda e_i : \lambda \in \mathbb{F}_p\}| = p$

Finalement le nbr de choix de bases possible est :

$$\prod_{k=1}^{n} (p^n - p^{k-1}) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

par construction $(e_1, \dots, e_n) \in \mathbb{F}_p{}^n \setminus \{0\} \times \mathbb{F}_p{}^n \setminus \mathbb{F}_p e_1 \times \cdots \times \bigoplus_{i=1}^{n-1} \mathbb{F}_p e_i$ et le cardinal de cet ensemble est le produit des cardinaux

Dc $|G| = \prod_{k=1}^{n} (p^n - p^{k-1})$

$= \prod_{k=1}^{n} p^{k-1} \times (p^{n-k+1} - 1)$

$= p^{\sum_{k=1}^{n}(k-1)} \times \prod_{k=1}^{n} (p^{n-k+1} - 1)$

$\sum_{l=0}^{n-1} l = \frac{(n-1)(n-1+1)}{2}$

$= p^{\frac{n(n-1)}{2}} \times m$

où $p \nmid m$

En général, pour $\alpha \in \mathbb{N}^*$
$p \nmid p^\alpha - 1$ car $p \mid p^\alpha - 1 \iff p^\alpha - 1 \equiv 0 [p]$
$\iff p^\alpha \equiv 1 [p]$

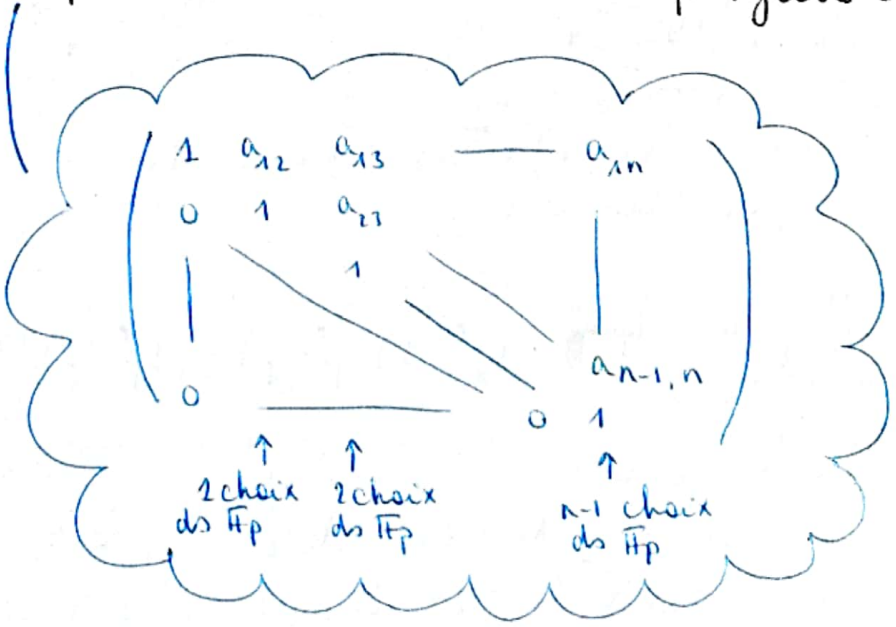
or $p \mid p^\alpha$ donc $p^\alpha \equiv 0 [p]$.

Ainsi chaque terme du produit de m n'est pas divisible par p et donc m non plus

Il suffit alors de remarquer que le sous-groupe des matrices triangulaires sup strictes de G que l'on note:

$$S = \{A = (a_{ij}) \in G : a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 0\}$$

est d'ordre $|S| = p^{\frac{n(n-1)}{2}}$ c'est donc un p-Sylow de G.



PREUVE DE SYLOW 1:

Soit G un groupe fini. Soit p un diviseur premier de $|G|$ tel que $n = |G| = p^\alpha m$ où $\begin{cases} p \nmid m \\ \alpha \in \mathbb{N}^* \end{cases}$

On mq G admet un sous-groupe S d'ordre p^α. Pour cela on va utiliser le fait que $Gl_n(\mathbb{F}_p)$ admet un p-Sylow.

En fait on montre:

(I) [Lemme] "Si un groupe admet un Sylow alors ses sous-groupes aussi"

> Soit K un groupe fini. Soit S un p-Sylow de K
> Soit H un sous-groupe de K.
> ALORS: il existe $a \in K$ tq: $aSa^{-1} \cap H$ est un p-Sylow de H

(II) G s'identifie à un sous-groupe de $Gl_n(\mathbb{F}_p)$

Puisque $Gl_n(\mathbb{F}_p)$ admet un Sylow, si G est un sous-gpe de $Gl_n(\mathbb{F}_p)$ par le lemme on a le résultat voulu.

Preuve de (I):

On cod l'action par conjugaison:

$$\begin{array}{ccc} K \curvearrowright K/S & \longrightarrow & K/S \\ (g, aS) & \longmapsto & gaS \end{array}$$

Puisque H est un sous-groupe de K cette action en induit une autre:

$$\begin{array}{ccc} H \curvearrowright K/S & \longrightarrow & K/S \\ (h, aS) & \longmapsto & haS \end{array}$$

On remarque que: $Stab_K(aS) = aSa^{-1} \quad \forall a \in K$

En effet, soit $a \in K$

$$\begin{aligned} \mathrm{Stab}_K(aS) &= \{g \in K : gaS = aS\} \\ &= \{g \in K : \bar{a}^1 g a S = S\} \\ &= \{g \in K : \bar{a}^1 g a \in S\} \\ &= aS\bar{a}^1 \end{aligned}$$

En général, si $H \subset G$:
$\forall g \in G \ (gH = H \Leftrightarrow g \in H)$

Alors on en déduit que : pour tout $a \in K$:

$$\begin{aligned} \mathrm{Stab}_H(aS) &= \mathrm{Stab}_K(aS) \cap H \\ &= aS\bar{a}^1 \cap H \end{aligned}$$

$G \curvearrowright X \longrightarrow X$ et $H \leq G$
$(g, x) \mapsto g \cdot x$

$\mathrm{Stab}_H(x) = \{h \in H : h \cdot x = x\}$
$= \{g \in G : g \in H \text{ et } g \cdot x = x\}$
$= H \cap \mathrm{Stab}_G(x)$

Il nous faut donc montrer qu'il existe $a \in K$ tq

$\mathrm{Stab}_H(aS)$ est un p-Sylow de H, cad, il existe $a \in K$ tq :

① $\mathrm{Stab}_H(aS)$ est un p-groupe

② $p \nmid [H : \mathrm{Stab}_H(aS)]$

Pour $|G| = p^\alpha \cdot m$
$S \leq G$ p-Sylow de G
ssi $\begin{cases} S \text{ } p\text{-groupe} \\ p \nmid [G : S] = m \end{cases}$

① est vrai pour tout $a \in K$. En effet, soit $a \in K$.

$$\mathrm{Stab}_H(aS) = aS\bar{a}^1 \cap H \leq aS\bar{a}^1$$

De l'ordre de $\mathrm{Stab}_H(aS)$ divise celui de $aS\bar{a}^1$. Or $|aS\bar{a}^1| = |S|$ et S est un p-groupe. De $\mathrm{Stab}_H(aS)$ est un p-groupe

Lagrange

$\varphi_a : S \longrightarrow aS\bar{a}^1$ bijection
$x \longmapsto axa^1$

On montre ② par l'absurde. Supposons que pour tout $a \in K$ $p \mid [H : Stab_H(aS)]$. Alors $p \mid |{}^H/_{Stab_H(aS)}| = |Orb_H(aS)|$

$[G:H] = |{}^G/_H|$ par déf

En général, $G \curvearrowright X$
$\forall x \in X \quad \varphi_x : {}^G/_{Stab_G(x)} \longrightarrow G \cdot x$
$\bar{g} \longmapsto g \cdot x$
est une bijection

Or les orbites partitionnent l'ensemble sur lequel le groupe agit donc ici :

$$|Orb_H(aS)| \;\Big|\; |{}^K/_S| = [K:S]$$

Donc : $p \mid [K:S]$ ce qui contredit que S est un p-Sylow de K.

S p-Sylow de K
$\Rightarrow \begin{cases} |K| = p^\beta \cdot [K:S] \\ |S| = p^\beta \\ p \nmid [K:S] \end{cases}$

Preuve de (II) :

G est un groupe fini alors par le thme de Cayley il s'injecte dans $\mathfrak{S}_n$

En effet, note $G = \{g_1, \dots, g_n\}$ avec g_i deux à deux distincts. Comme G agit sur lui-même par translation à gauche cette action induit un mph :

$$\varphi : G \longrightarrow \mathfrak{S}(G)$$
$$g \longmapsto (\varphi_g : g_i \longmapsto g g_i = g_j)$$

Ce mph est injectif et comme $|G| = n$, $\mathfrak{S}(G) \simeq \mathfrak{S}_n$

Reste à remarquer que $\mathfrak{S}_n$ s'injecte dans $Gl_n(\mathbb{F}_p)$. On pose :

$$f : \mathfrak{S}_n \longrightarrow Gl_n(\mathbb{F}_p)$$
$$\sigma \longmapsto \left(f_\sigma : e_i \longmapsto e_{\sigma(i)} \right)$$

où $(e_i)_{1 \leq i \leq n}$ est la base canonique de $(\mathbb{F}_p)^n$.

Alors f est un morphisme et elle est injective

Ainsi on a :

$$G \xhookrightarrow{\varphi} \mathfrak{S}(G) \simeq \mathfrak{S}_n \xhookrightarrow{f} Gl_n(\mathbb{F}_p)$$

Donc G est isomph à un sous-groupe de $Gl_n(\mathbb{F}_p)$

$\phi : G \hookrightarrow G'$ mph de groupe
$\phi(G) \leq G'$ ss $\widetilde{\phi} : G \longrightarrow \phi(G)$ mph bijectif
Donc $G \simeq \phi(G) \leq G'$

PREUVE DE SYLOW 2 :

Soit G groupe fini et p premier tq $|G| = n = p^k m$ avec $p \nmid m$.

Soit H, S deux p-Sylow de G. On veut qu'il existe $a \in G$ tq $H = aSa^{-1}$.

En particulier $H \leq G$. Comme S est un Sylow, par le lemme ①, il existe $a \in G$ tel que : $aSa^{-1} \cap H$ est un p-Sylow de H. Or H est un p-groupe donc on a :

$$aSa^{-1} \cap H = H$$

$|H| = p^k$ donc un p-Sylow de H est de même cardinal que H. C'est donc H lui-même

De : $H \subset aSa^{-1}$. Or $|aSa^{-1}| = |S| = |H|$

S et H 2 p-Syl de G

De $H = aSa^{-1}$.