

Théorèmes de Sylow

Lemme 1: Soit $G = GL_n(\mathbb{F}_p)$, $S = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & * \end{pmatrix} \in G$, alors S est un p -Sylow de G .

On calcule $|G|$, ie on compte les bases $(e_i)_{i=1}^n$ de $\mathbb{F}_p^n$. Pour e_1 , on a $|\mathbb{F}_p^n / \langle e_1 \rangle| = p^{n-1}$ choix. Et $\forall k \in \{2, \dots, n\}$ on a $|\mathbb{F}_p^n / \bigoplus_{i=1}^{k-1} \mathbb{F}_p e_i| = p^{n-k+1}$ choix. Donc $|G| = \prod_{k=1}^n p^{n-k+1} = \prod_{k=1}^n p^{k-1} = p^{\frac{n(n-1)}{2}}$ ou p^m . Puisque $|S| = p^{\frac{n(n-1)}{2}}$, S est un p -Sylow de G .

Lemme 2: Soit $|G| = p^m m$, $p \nmid m$, $H < G$ et $S < G$ p -Sylow. Alors $\exists a \in G$, $aSa^{-1} \cap H$ p -Sylow de H .

On fait agir H sur G/S par translation à gauche. Alors, $\forall a \in G/S$ et $g \in H$ on a $g \in \text{Stab}(aS) \Leftrightarrow g \cdot aS = (ga)S = aS \Leftrightarrow a^{-1}ga \in S$. Donc $\text{Stab}(aS) = aSa^{-1} \cap H$. De plus, on a $|G/S| = |\sum \text{Orb}| = \frac{|G|}{|S|} = m$, donc $\exists a \in G$ tel que $p \nmid |\text{Orb}(aS)|$. Alors $p \nmid \frac{|H|}{|aSa^{-1} \cap H|} = [H : aSa^{-1} \cap H]$ et puisque $aSa^{-1} \cap H < aSa^{-1}$, c'est un p -groupe. D'où $aSa^{-1} \cap H$ p -Sylow de H .

Théorème: Soit $|G| = n = p^m m$, $p \nmid m$. ① G contient un p -Sylow; ② Si $H < G$ p -groupe, alors

$\exists S < G$ p -Sylow, $H \subset S$; ③ les N_p p -Sylow sont 2 à 2 conjugués dans G ; ④ $N_p \cong 1 \text{ Cp}$ et $N_p \mid m$.

① Par Cayley, $G \hookrightarrow Y_n$. Puisque $Y_n \hookrightarrow GL_n(\mathbb{F}_p)$, on a $G \hookrightarrow GL_n(\mathbb{F}_p)$. Par les lemmes, G admet un p -Sylow.

② Soit $H < G$ p -groupe et $S < G$ p -Sylow. Par le lemme 2, $\exists a \in G$ tel que $aSa^{-1} \cap H$ p -Sylow de H .

Or H p -groupe, donc $aSa^{-1} \cap H = H$ et $H \subset aSa^{-1}$, qui est un p -Sylow de G .

③ Si de plus H est un p -Sylow de G , on a $|H| = |S| = |aSa^{-1}|$ donc $H = aSa^{-1}$.

④ Soit X l'ensemble des p -Sylow de G et $S \in X$. On fait agir S sur X par conjugaison. On a $X^S = \{T \in X \mid \forall s \in S, sTs^{-1} = T\} = \{T \in X \mid \text{Orb}(T) = \{T\}\}$, donc l'équation aux classes donne $N_p = |X| = |X^S| + \sum_{|\text{Orb}| > 1} |\text{Orb}|$. Or, $|\text{Orb}| \mid |S| = p^m$, donc si $|\text{Orb}| > 1$, on a $p \mid |\text{Orb}|$. D'où $N_p \equiv |X^S| \pmod{p}$.

④ Soit $T \in X^S$ et $N = \langle T, S \rangle$. Puisque $T, S < N$, ce sont des p -Sylow de N . De plus, $\forall n \in N$, $nTn^{-1} = T$ donc $T \trianglelefteq N$. Or, $\exists a \in N$ tel que $S = aTa^{-1} = T$, donc $X^S = \{S\}$. D'où $N_p \equiv 1 \pmod{p}$.

④ De plus, en faisant agir G sur X par conjugaison, il n'y a qu'une orbite par le point ③. Donc $\forall S \in X, |\text{Orb}(S)| = |X| \mid |G|$, ie $N_p \mid p^m m$. Or N_p premier avec p , donc $N_p \mid m$.

Définition: Soit G groupe, $|G| = n = p^\alpha m$ où p premier, $\alpha \in \mathbb{N}^*$, $p \nmid m$. Un p -sous-groupe de Sylow de G est $H < G$ tel que $|H| = p^\alpha$ (p -Sylow de G).

Remarque: $H < G$ p -Sylow $\Leftrightarrow H < G$ p -groupe et $p \nmid [G:H]$.

$(\Rightarrow)$ $|H| = p^\alpha$ donc H p -Groupe et $[G:H] = \frac{|G|}{|H|} = m$, $p \nmid m$. $(\Leftarrow)$ Si $|H| = p^\beta$, $\beta \in \mathbb{N}^*$ et $[G:H] = r$, alors $|G| = p^\beta m = [G:H]|H| = p^\beta r$. Donc $p^{\alpha-\beta} m = r$ où $p \nmid r$. Mais $\alpha = \beta$, $m = r$.

Définition: G agit sur X par $(g, x) \in G \times X \mapsto g.x \in X$. On note $\forall x \in X$

$\text{Orb}(x) = \{g.x \mid g \in G\}$, $\text{Stab}(x) = \{g \in G \mid g.x = x\} < G$, $X^G = \{x \in X \mid g.x = x \forall g \in G\}$

Remarque: $X^G = \{x \in G \mid \text{Orb}(x) = \{x\}\} = \{x \in G \mid |\text{Orb}(x)| = 1\}$

Théorème: Si $|G| = n$, alors $G \hookrightarrow \mathcal{P}_n$

G agit sur G par translation à gauche, $(g, x) \in G \times G \mapsto g.x = gx \in G$, associée au morphisme $\varphi: G \rightarrow \mathcal{P}(G)$. Soit $g \in \text{Ker } \varphi$, on a $\forall x \in G$ $\varphi(g)(x) = g.x = gx = x$, donc en $x = e$, $g = e$ et φ injectif. Puisque $\mathcal{P}(G) \cong \mathcal{P}_n$, on a $G \hookrightarrow \mathcal{P}_n$.

Théorème: $\mathcal{P}_n \hookrightarrow \text{GL}_n(\mathbb{F}_p)$

Soit $\varphi: \sigma \in \mathcal{P}_n \mapsto \varphi(\sigma) \in \text{GL}_n(\mathbb{F}_p)$, où $\varphi(\sigma): e_i \in \mathbb{F}_p^n \mapsto \sigma(e_i) \in \mathbb{F}_p^n$ avec $(e_i)_{1 \leq i \leq n}$ base canonique de $\mathbb{F}_p^n$. On a bien $\varphi(\sigma) \in \text{GL}_n(\mathbb{F}_p)$ car envoie base sur base de $\mathbb{F}_p^n$. On a

$\forall \sigma, \tau \in \mathcal{P}_n$, $\forall i \in [1, n]$ $\varphi(\sigma\tau)(e_i) = \sigma\tau(e_i) = \sigma(\tau(e_i)) = \varphi(\sigma)(\tau(e_i)) = \varphi(\sigma)(\varphi(\tau)(e_i))$.

D'où $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$. Si $\sigma \in \text{Ker } \varphi$, on a $\forall i \in [1, n]$ $\sigma(e_i) = e_i$, i.e. $\sigma = \text{Id}$ et φ inj.

Proposition: Soit $x \in X$. Alors $\varphi_x: \bar{g} \in G/\text{Stab}(x) \mapsto g.x \in \text{Orb}(x)$ bijection

Par définition de $\text{Orb}(x)$, $\varphi_x(\bar{g}) \in \text{Orb}(x)$. On a $\forall g, h \in G$

$\bar{g} = \bar{h} \Leftrightarrow g^{-1}h \in \text{Stab}(x) \Leftrightarrow g^{-1}h.x = x \Leftrightarrow h.x = g.x \Leftrightarrow \varphi_x(\bar{g}) = \varphi_x(\bar{h})$.

Donc φ_x bien définie (ne dépend pas du représentant) et injective. Par construction surjective.

Application: $|G| = 15 \Rightarrow G \cong \mathbb{Z}/15\mathbb{Z}$. $|G| = 63 \Rightarrow G$ pas simple

* $N_2 \equiv 1(3)$ et $N_2 \mid 15 \Rightarrow N_2 = 1$; $N_3 \equiv 1(5)$ et $N_3 \mid 3 \Rightarrow N_3 = 1$ et $S_2, S_5 \triangleleft G$ car seuls 3-Sylow et 5-Sylow. Comme $|S_2 \cap S_5| \mid 3 \wedge 5 = 1$, $S_2 \cap S_5 = \{e\} \Rightarrow G \cong S_2 \times S_5 \cong \mathbb{Z}/2\mathbb{Z} \times S_5$

* $63 = 7 \times 3^2$, $N_7 \equiv 1(7)$ et $N_7 \mid 9 \Rightarrow N_7 = 1$ et $\exists S_7 \triangleleft G$ 7-sylow