Théorème de Sylow

0) Terminology : l'action de $G \curvearrowright X$ est fidèle si g vérifie $gx = x$ pour tout x de G, alors $g = e$.

proposition : $G \curvearrowright X$ fidèle $\Leftrightarrow$ Morphisme d'action $G \to Bij(X)$ est injectif.

ex : les actions à droite et à gauche de $G \curvearrowright G$ sont fidèles.

1. Quelques groupes et sous-groupes importants

ⓐ le groupe $\mathfrak{S}_n = Bij\{1, \dots, n\}$

prop : tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$

◀ l'action à gauche de $G \curvearrowright G$ donne un morphisme $G \to Bij(G)$; $g \mapsto \phi_g$ où $\phi_g(h) = gh$. L'application ϕ est injective ! Si $\phi_g = Id$; alors $g = g \cdot e = \phi_g(e) = e$. ▶

ⓑ le groupe $GL(n, \mathbb{K})$ par un corps $\mathbb{K}$ de cardinal k

proposition : $\# GL_n(\mathbb{K}) = k^{n-1}(k^n - 1) \# GL_{n-1}(\mathbb{K})$

◀ Application de la formule des classes, vue en exercice ▶

proposition : il existe une injection de $\mathfrak{S}_n$ dans $GL_n(\mathbb{K})$

◀ $\sigma \in \mathfrak{S}_n \to$ l'endomorphisme ϕ_σ tel que $\phi_\sigma(e_i) = e_{\sigma i}$, où $(e_1, \dots, e_n)$ est une base de $\mathbb{K}^n$ ▶

Corollaire : Pour tout groupe fini G d'ordre n, pour tout corps $\mathbb{K}$, il existe une injection de G dans $GL(n, \mathbb{K})$

« Pour tout corps, $\mathbb{K}$ un groupe d'ordre n est un sous groupe de $GL_n(\mathbb{K})$ »

ⓒ le groupe $B_n(\mathbb{K}) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} < GL_n(\mathbb{K})$

◀ Groupe : $g(e_1) = e_1$; $g(e_j) = e_j + u_j$ avec $u_j \in P_{j-1} = \langle e_1, \dots, e_{j-1} \rangle$

$\Rightarrow$ si $g, h \in P_j$ alors $g \cdot h \in B_n(\mathbb{F}_p)$

Inverse $g(g^{-1}(e_j)) = e_j$; donc $g^{-1}(e_j) \in P_j$

écrivons $g^{-1}(e_j) = \alpha \cdot e_j + u_j \Rightarrow \alpha e_j + \underbrace{g(u_j)}_{\in P_{j-1}} + u_j = e_j \Rightarrow \alpha = 1$

2. Sous groupes de Sylow

Soit G un groupe d'ordre n, Soit p un nombre premier et supposons $n = p^\alpha q$ avec q premier avec p

Un p groupe de G est un sous groupe d'ordre p^m avec p premier

Un p-groupe de Sylow est un sous groupe de G d'ordre p^α

prop Soit S un p-groupe agissant sur X alors

$\#X \equiv n\ [p]$ où n = nombre de pt fixes de l'action de S (i.e orbite réduite à un point) sur P

Exemple :

$G = GL_n(\mathbb{F}_{p^m})$ les matrices triangulaires supérieures forment un p-groupes de Sylow.

◀ Si $\mathbb{F}$ est de cardinal $k = p^m$, alors on a vu que $\#GL_n(F) = k^{n-1}(k^n - 1)\#GL_{n-1}(k)$; Démontrons ceci par récurrence que

supposons $\#GL_n(F) = k^{\frac{n(n-1)}{2}} \cdot q_n$ avec q_n premier avec p.

Alors $\#GL_{n+1}(F) = k^{n+1+\frac{(n+1)(n}{2}} \cdot q_n \cdot (k^{n+1} - 1)$.

Comme $n + \frac{n(n-1)}{2} = \frac{1}{2}(n(n+1))$ et $(k^{n+1} - 1) \equiv 1\ [p]$, le résultat est démontré par récurrence. Maintenant $\#B_n(\mathbb{F}) = k^{\frac{n(n-1)}{2}}$. le résultat suit ▶

Remarque : si H est un p-groupe, ou un p-groupe de Sylow tout conjugué de H est un p-groupe (de Sylow)

◀ Si $\alpha \in G$, la conjugaison $u \mapsto \alpha u \alpha^{-1}$ est une bijection ▶

3. Le Théorème de Sylow

Theorème : Si G est d'ordre $p^\alpha q$ avec p premier et q premier avec p alors

(i) G contient un p-groupe de Sylow

(ii) tout les p-groupes de Sylow sont conjugués

(iii) tout p-groupe est inclus dans un groupe de Sylow

(iv) le nombre n_p de p-Sylow est $\equiv 1[p]$ et divise q

Corollaire de (ii) : si un p-Sylow est distingué c'est l'unique p Sylow. (*)

On commence par

① Soit F un groupe ayant S comme p groupe de Sylow, Soit $G<F$, alors il existe α tel que $G \cap \alpha S \alpha^{-1}$ est un p-groupe de Sylow de G

◀ On considère $X = F/S$, par construction si $\#F = p^\alpha q$ avec q premier avec p alors $\#X = q$; On fait agir G à gauche sur F/S

$$(h, xS) \mapsto hxS$$, il s'agit bien d'une action

$$\mathrm{Stab}(xS) = \{h \mid hxS = xS\} = \{h \mid x^{-1}hx S = S\} = \{h \mid x^{-1}hx \in S\}$$
$$= G \cap x^{-1}Sx < x^{-1}Sx,$$ c'est un p-groupe de G

Si $\mathrm{Stab}(xS)$ n'est pas un p-groupe de Sylow alors $p \mid \#G(xS)$

· Nous pouvons raisonner par contradiction : si

$G \cap xSx^{-1}$ n'est jamais un p-Sylow, alors p divise le cardinal de toutes les orbites et donc $p \mid \#X$ et la contradiction ▶

Demonstration de (i) : on applique le lemme à l'injection de $G \hookrightarrow GL_n(\mathbb{F}_p)$ qui possède un p-Sylow.

Demonstration de (ii) et (iii) Soit $H < G$ un p-groupe ; Soit S un p-Sylow de G

On sait qu'il existe x tel que $H \cap xSx^{-1}$ est un p-Sylow de H, or

H est son propre p-Sylow donc $H \subset xSx^{-1}$.

En particulier si S' est un autre p-Sylow $S' \subset xSx^{-1}$ et comme

S' et xSx^{-1} ont le m̂ cardinal, ils sont egaux.

Demonstration de (iv).

Soit $X = \{p\text{-Sylow}\}$; alors on fait agir G par conjugaison sur X. On observe tout d'abord.

Si $S_0 \in X$, Alors $S_0 \lhd Stab(S_0)$. En particulier

(i) S_0 est l'unique p-Sylow de $Stab(S_0)$

(ii) $S_0 < Stab(S) \cap S_0 \Rightarrow S = S_0$

◀ pour tout x de S_0, on a $xS_0x^{-1} = S_0$; donc $x \in Stab(S_0)$.
Par ailleurs, par definition pour tout y de $Stab(S_0)$, $yS_0y^{-1} = S_0$
donc $S_0 \lhd Stab(S_0)$. (i) est alors une consequence du corollaire. (*).
Si maintenant $S_0 < Stab(S)$. Alors S_0 est un p-Sylow de $Stab(S)$ donc par (i)
$S = S_0$ ▶

Comme $S_0 < Stab(S_0)$, $\# Stab(S_0) = q'p^{\alpha}$. De plus, comme tous les p-Sylow sont conjugués. $\# X = \# G / \# Stab(S_0) =: n_p$

donc $n_p q' = q$: n_p divise q

On fait agir $S_0 \circlearrowright X$ par conjugaison, le stabilisateur de S par cette action est $Stab(S) \cap S_0$. On vient de montrer que X a une seule orbite triviale donc $\# X \equiv 1 \, [p]$

pourquoi ?