Théorèmes de Sylow

Dorian Cacitti-Holland

2020-2021

Références.

1. Cours d'algèbre de Daniel Perrin

Leçons.

1. 101 Groupe opérant sur un ensemble, exemples et applications
2. 103 Conjugaison dans un groupe, exemples de sous-groupes distingués et de groupes quotients, applications
3. 104 Groupes abéliens et non abéliens finis, exemples et applications
4. 106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$, applications
5. 121 Nombres premiers, applications
6. 123 Corps finis, applications

Lemme. (Seulement pour les leçons 106 et 123) Soit G un groupe de cardinal n, alors G isomorphe à un sous-groupe de S_n, donc à un sous-groupe de $GL_n(\mathbb{F}_p)$.

Démonstration.
On considère l'application

$$\varphi : \begin{array}{ccc} G & \longrightarrow & S(G) \simeq S_n \\ g & \longmapsto & [h \longmapsto gh] \end{array}$$

Alors φ est un morphisme de groupes injectif car

$$\forall (g_1, g_2) \in G^2, \forall h \in G, \varphi(g_1g_2)(h) = (g_1g_2)h = g_1(g_2h) = (\varphi(g_1) \circ \varphi(g_2))(h)$$

Et

$$\forall g \in G, \varphi(g) = id_G \Rightarrow \forall h \in G, gh = h \Rightarrow g = 1$$

D'où $G \simeq \varphi(G)$ sous-groupe de S_n lui-même sous-groupe de $GL_n(k)$ avec $k = \mathbb{F}_p$ via les matrices de permutations.
En effet l'application suivante

$$\psi : \begin{array}{ccc} S_n & \longrightarrow & GL_n(\mathbb{F}_p) \\ \sigma & \longmapsto & \left(e_{\sigma(1)} \mid ... \mid e_{\sigma(n)}\right) \end{array}$$

est un morphisme de groupes injectif :

— On a bien $\psi(id) = I_n$ car

$$\forall x = \sum_{i=1}^{n} x_i e_i \in \mathbb{F}_p^n, \psi(\sigma)x = \sum_{i=1}^{n} x_i \psi(\sigma) e_i = \sum_{i=1}^{n} x_i e_i = x$$

— Soit $\sigma, \tau \in S_n$, alors, pour tout $i, j \in [\![1, n]\!], (\psi(\sigma\tau))_{ij} = \delta_{i,\sigma(\tau(j))} = \delta_{i,\sigma(j)}\delta_{j,\tau(j)}$ et

$$(\psi(\sigma)\psi(\tau))_{ij} = \sum_{k=1}^{n} \psi(\sigma)_{ik}\psi(\tau)_{kj} = \sum_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{k,\tau(j)} = \delta_{i,\sigma(\tau(j))} = (\psi(\sigma\tau))_{ij}$$

D'où $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$.

— Soit $\sigma \in S_n$, alors, pour tout $i, j \in [\![1, n]\!]$,

$$(\psi(\sigma)\psi(\sigma^{-1}))_{ij} = \sum_{k=1}^{n} \delta_{i,\sigma(k)}, \delta_{k,\sigma^{-1}(j)} = \delta_{i,\sigma(\sigma^{-1}(j))} = \delta_{ij}$$

D'où $\psi(\sigma)\psi(\sigma^{-1}) = I_n$, ie $\psi(\sigma^{-1}) = \psi(\sigma)^{-1}$.

— Soit $\sigma \in S_n$ tel que $\psi(\sigma) = I_n$, alors

$$n = tr(\psi(\sigma)) = \sum_{i=1}^{n} \psi(\sigma)_{ii} = \sum_{i=1}^{n} \delta_{i,\sigma(i)}$$

Ainsi, comme δ est à valeurs dans $\{0, 1\}$, $\forall i \in [\![1, n]\!], i = \sigma(i)$, ie $\sigma = I_n$ ce qui montre que ψ est injectif.

□

Lemme. (Seulement pour les leçons 106 et 123) L'ensemble T des matrices triangulaires supérieures de diagonale unitaire est un p-Sylow de $GL_n(\mathbb{F}_p)$.

Démonstration.
On a

$$|T| = |\mathbb{F}_p|^{\sum_{i=1}^{n-1} i} = p^{\frac{n(n-1)}{2}}$$

Or, en dénombrant les bases de $\mathbb{F}_p^n$,

$$|GL_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i) = \prod_{i=0}^{n-1} p^i(p^{n-i} - 1) = p^{\sum_{i=0}^{n-1} i} \prod_{i=1}^{n}(p^i - 1) = p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(p^i - 1)$$

Avec p ne divisant pas $\prod_{i=1}^{n}(p^i - 1)$.
D'où T est un p-Sylow de $GL_n(\mathbb{F}_p)$. □

Théorême. Premier théorème de Sylow : Soit G un groupe fini et $p \in \mathcal{P}$ divisant $|G|$, alors G admet un p-Sylow.

Démonstration.
Soit $G' = GL_n(\mathbb{F}_p)$ groupe de cardinal $|G'| = p^\alpha m$ avec m, p premiers entre eux.
Par théorème de Cayley on a $G < S_n < G'$ (à isomorphisme près).
Soit S le sous-groupe de $GL_n(\mathbb{F}_p)$ des matrices triangulaires supérieures de diagonale unitaire, alors S est un p-Sylow de G'.
On fait agir G' sur l'ensemble G'/S par translation à gauche :

$$\forall (g, aS) \in G' \times G'/S, g.aS = (ga)S$$

Alors, pour $aS \in G'/S$, le stabilisateur de aS est

$$Stab_{G'}(aS) = \{g \in G', (ga)S = g.aS = aS\} = \{g \in G', \exists (s_1, s_2) \in S^2, gas_1 = as_2\} = aSa^{-1}$$

Or par restriction G agit également sur G'/S avec comme stabilisateur, pour $aS \in G'/S$,

$$Stab_G(aS) = aSa^{-1} \cap G$$

Or $aSa^{-1} \cap G$ est un p-sous-groupe de G comme sous-groupe du p-Sylow aSa^{-1}. On suppose par l'absurde que pour tout $aS \in G'/S$,

$$p \mid |G/(aSa^{-1} \cap G)|$$

Or $G'/S = \bigsqcup_{aS \in G'/S} Orb_G(aS)$ et, par relation orbite-stabilisateur, on a

$$|G/(aSa^{-1} \cap G)| = |G/Stab_G(aS)| = |Orb_G(aS)|$$

Donc

$$p \mid \sum_{aS \in G'/S} |Orb_G(aS)| = |G'/S| = m$$

Ce qui est absurde.
Par conséquent il existe $aS \in G'/S$ tel que $|G/(aSa^{-1} \cap G)|$ soit premier avec p, d'où $aSa^{-1} \cap G$ est un p-Sylow de G car $|G| = |aSa^{-1} \cap G|\,|G/(aSa^{-1} \cap G)|$. $\square$

Théorème. (Sauf pour les leçons 106 et 123) **Second théorème de Sylow :** Soit G un groupe de cardinal $|G| = p^\alpha m$ avec $p \in \mathcal{P}, \alpha \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ tel que p ne divise pas m, alors :

1. Soit H un p-groupe de G, alors il existe un p-Sylow S tel que $H \subset S$.
2. Les p-Sylow sont tous conjugués, donc leur nombre $n_p \mid n$.
3. $n_p \equiv 1[p]$ donc $n_p \mid m$.

Démonstration.
Etape 1 : Démonstration de 1
Soit H un p-sous-groupe de G et S un p-Sylow de G, alors d'après la démonstration précédente, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.
Or H est un p-groupe, donc

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

Ainsi

$$H \subset aSa^{-1}$$

Avec aSa^{-1} un p-Sylow ce qui montre i.
Etape 2 : Les p-Sylow sont conjugués
De plus si H est un p-Sylow alors on a

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

D'où les p-Sylow sont tous conjugués.
Etape 3 : $n_p \mid n$
On considère l'action de G sur l'ensemble des sous-groupes de G par conjugaison.
Ainsi, d'après ce qui précède, les p-Sylow sont dans une orbite commune de carinal n_p, d'où d'après la relation orbite-stabilisateur

$$n_p \mid n$$

Etape 4 : $n_p \equiv 1[p]$
On considère l'action de G par conjugaison sur l'ensemble X des p-Sylow de G.
Soit S un p-Sylow de G, alors S agit par restriction sur X.
Ainsi

$$|X| \equiv |X^S|[p]$$

avec $X^S := \{T \in X, \forall s \in S, sTs^{-1} = T\}$.
Soit $T \in X^S$, on considère le sous-groupe N de G engendré par S et T.
Ainsi S et T sont des sous-groupes de N, donc en particulier S et T sont des p-Sylow de N, d'où, d'après ce qui précède, T et S sont conjugués dans N, ie il existe $n \in N$ tel que

$$S = nTn^{-1}$$

De plus, comme S et T normalisent T et engendrent N, $T \triangleleft N$.
Par conséquent $S = T$ ce qui montre que $|X^S| = 1$ puis

$$n_p = |X| \equiv 1[p]$$

□

Lemme. (Seulement s'il reste du temps) Soit G un p-groupe agissant sur un ensemble X et $X^G = \{x \in X, \forall g \in G, g.x = x\}$ l'ensemble des points fixes de X sous G, alors

$$|X| \equiv |X^G|[p]$$

Démonstration.
Pour tout $x \in X$,

$$x \in X^G \iff Orb_G(x) = \{x\}$$

Donc si $x \notin X^G$, $|Orb_G(x)| > 1$, de plus $|Orb_G(x)| \mid p^n$ donc $p \mid |Orb_G(x)|$.
Par conséquent

$$|X| = |X^G| + \sum_{x \in X \setminus X^G} |Orb_G(x)| \equiv |X^G|[p]$$

□