Théorème de Sylow

Nico

Prérequis : Théorème de Cayley

Notations :

1. Etant donné un groupe G et un partie X, on note $N_G(X) = \{g \in G : gXg^{-1} = X\}$ le normalisateur de X dans G.

Définition H est un p-sous-groupe de G si $|H|$ est une puissance de p, et $[G : H] \wedge p = 1$.

Définition Soit G un groupe fini d'ordre $n = p^\alpha m$, p premier, $\alpha \geq 1$ et $p \nmid m$. Alors G admet un p-sous-groupe d'ordre p^α, qu'on appelle p-Sylow.

Lemme : Soit G un groupe fini d'ordre $p^\alpha m$, p premier, $\alpha \geq 1$ et $p \nmid m$ et H un sous-groupe de G. Si G admet un p-Sylow S, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Démonstration. Montrons qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

On fait agir G sur G/S par :

$$\forall g \in G,\ \forall x \in G,\ g \cdot xS = gxS$$

Soit $a \in G$,

$$Stab(aS) = \{g \in G : gaS = aS\} = \{g \in G : \exists x, y \in S,\ g = axy^{-1}a^{-1}\} = aSa^{-1}$$

Mais H opère aussi sur G/S, d'où par restriction, le stabilisateur pour l'action de H sur G/S est $aSa^{-1} \cap H$, qui est donc un sous-groupe de H. Il reste à montrer que pour un certain a, il s'agit d'un p-Sylow.

Il est clair qu'il s'agit d'un p-groupe, puisque S en est un et que tout groupe conjugué à un p groupe, est un p groupe [(1)] $++$. Trouvons $a \in G$ tel que $|H/(aSa^{-1} \cap G)|$ soit premier à p.

(1). Considérer l'application $S \to gSg^{-1}$, $s \mapsto gsg^{-1}$, et montrer qu'elle est bijective

Par équations des classes :

$$|H/(aSa^{-1} \cap H)| = |Orb(aS)|$$

Où $Orb(aS)$ est l'orbite de aS dans G/S sous l'action de H. Si pour tout $a \in G$, $p \mid |Orb(aS)|$, alors $p \mid |G/S|$ puisque les orbites forment une partition. Ce qui n'est pas possible puisque S est un $p-$Sylow de G. D'où il existe a tel que $p \nmid |Orb(aS)|$. □

Soit G un groupe fini d'ordre $p^\alpha m$, p premier, $\alpha \geq 1$ et $p \nmid m$. Alors :

1. **Premier théorème de Sylow** : G admet un p-Sylow
2. **Deuxième théorème de Sylow :** Notons n_p le nombre de p-Sylow de G.
   (a) Si $H \leq G$ est un p-groupe, il existe un p-Sylow S de G tel que $H \leq S$. De plus, Les p-Sylow de G sont tous conjugués.
   (b) $n_p \mid n$, $n_p \equiv 1 \pmod p$, et donc $n_p \mid m$.

Montrons le premier point :

Démonstration. Le théorème de Cayley nous donne que G est isomorphe à un sous-groupe de $\mathfrak{S}_n$, qui est lui-même isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$. Commençons alors par étudier le groupe $H = GL_n(\mathbb{F}_p)$.
On sait que :
$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1) \dots (p - 1)$.
On a que $\alpha = \dfrac{n(n-1)}{2}$ et $m = (p^n - 1)(p^{n-1} - 1) \dots (p - 1)$, qui n'est bien pas divisible par p. Or le sous-groupe de H formé des matrices triangulaires supérieurs avec des 1 sur la diagonale de cardinal p^α. H admet donc un p-Sylow.
Ainsi, G est sous-groupe d'un groupe isomorphe à $GL_n(\mathbb{F}_p)$ qui admet un p-Sylow. D'où par lemme, G admet un p-Sylow. □

Montrons le deuxième point :

Démonstration. Montrons que si H est un sous-groupe de G et un p-groupe, alors il existe un p-Sylow S tel que $H \subseteq S$.

Soit S un p-Sylow de G. Par le lemme, on considère $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Alors $aSa^{-1} \cap H \leq H$ et par égalité des cardinaux, $H = aSa^{-1} \cap H$ car H est un p-groupe. Donc $H \subseteq aSa^{-1} =: S'$, qui est un p-Sylow [(2)].

(2). On a égalité des cardinaux, toujours par la bijection entre S et aSa^{-1}

Si de plus H est un p-Sylow, alors $H = aSa^{-1}$. Ainsi, tous p-Sylow sont conjugués entre eux. $\square$

Montrons le troisième :

Démonstration. Notons X l'ensemble des p-Sylow de G. On fait agir G par conjugaison sur cet ensemble :

$$\forall g \in G,\ \forall S \in X,\ g \cdot S = gSg^{-1}$$

Par le point précédent, l'action est transitive. En effet, pour tout $S \in X$, S est conjugué avec tous les autres p-Sylow. D'où $Orb(S) = X$. Le stabilisateur de S est par définition, son normalisateur. D'où l'équation des classes fournit le premier résultat souhaité :

$$n_p = |X| = |G/N_G(S)| = [G : N_G(S)]$$

Et on a bien que $|X| \mid |G| = n$.

Montrons que $n_p \equiv 1 \pmod p$. Soit S un p-Sylow de G. On fait agir S par conjugaison sur X. Soit $X^S = \{S' \in X : \forall s \in S,\ sS's^{-1} = S'\}$. On sait que X^S contient exactement tous les éléments d'orbites de cardinal 1, d'où l'équation aux classes fournit que :

$$|X| \equiv |X^S| \pmod p$$

Car S est un $p-$groupe. Montrons que $|X^S| = 1$. **J'ai choisi de ne pas faire comme le Perrin pour cette preuve :**

D'une part, $S \in X^S$ par clôture du groupe S. Soit T un p-Sylow de G différent de S. Supposons par l'absurde que $T \in X^S$. Soit $N_G(T) = \{g \in G : gTg^{-1} = T\}$. Pour tout $s \in S$, $sTs^{-1} = T$, alors pour tout $s \in S$, $s \in N_G(T)$. Donc $S \subseteq N_G(T)$. Mais aussi, $T \subseteq N_G(T)$. Donc S et T sont deux p-Sylow de $N_G(T)$ car $N_G(T)$ est sous-groupe de G. Finalement

1. Par le premier point, tous les p-Sylow de $N_G(T)$ sont conjugués. Donc il existe $g \in N_G(T)$ tel que $gTg^{-1} = S$.
2. Par définition de $N_G(T)$, $gTg^{-1} = T$.
3. D'où $S = T$

D'où $n_p \equiv 1 \pmod p$. Entre autre $n_p \nmid p^\alpha$, donc $n_p \mid m$. $\square$

Je démontre maintenant quelques résultats annexes :

1. Soit $q = p^\alpha$, calculons le cardinal de $|GL_n(\mathbb{F}_q)$: Calculons pour cela le nombre de bases dans $\mathbb{F}_q^n$. Soit B une base de $\mathbb{F}_q^n$

(a) v_1 est élément de B si $v_1 \neq 0$: $q^n - 1$ choix.

(b) Si v_1 est élément de B, v_2 est élément de B si v_1 et v_2 ne sont pas colinéaires : $q^n - q$ choix.

(c) Si $v_1, \dots, v_i$ sont éléments de B, v_{i+1} est élément de la base n'appartient pas à $\mathrm{Vect}(v_1, \dots, v_i)$: $q^n - q^i$ choix.

Finalement, le nombre de bases est :

$$(q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\dots(q - 1)$$

C'est aussi le cardinal de $GL_n(\mathbb{F}_q)$.

2. Montrons le théorème de Cayley : Soit G un groupe fini d'ordre n. On fait agir G sur lui même par translation à gauche :

$$\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(G) \\ g & \longmapsto & \varphi_g : \left\{ \begin{array}{ccc} G & \to & G \\ h & \mapsto & gh \end{array} \right. \end{array} \right.$$

Il s'agit d'un morphisme de groupe. Montrons qu'il est injectif (ie que l'action est fidèle). Soit $g \in G$ tel que :

$$\forall h \in G,\ gh = h$$

Alors $g = e$ par définition du neutre. D'où G s'injecte dans $\mathfrak{S}(G) \simeq \mathfrak{S}_n$.

3. Montrons que $\mathfrak{S}_n$ s'injecte dans $GL_n(\mathbb{K})$, où $\mathbb{K}$ est un corps quelconque. Considère l'application $\theta : \sigma \mapsto P_\sigma$, où $\sigma \in \mathfrak{S}_n$ et P_σ est une matrice de permutation. Montrons qu'elle est injective. Soit $\sigma \in \mathfrak{S}_n$. Soit $u \in GL(\mathbb{K}^n)$ l'endomorphisme associé à P_σ pour la base canonique de $\mathbb{K}^n$, noté $(e_1, \dots, e_n)$. Alors $u(e_i) = e_{\sigma(i)}$. Montrons que l'application est un morphisme de groupe. $\theta(\mathrm{Id}) = I_n$ très clairement, et soient $\sigma, \tau \in \mathfrak{S}_n$ et u, v les endos associés. Alors pour tout i :

$$(u \circ v)(e_i) = u(v(e_i)) = e_{\sigma(\tau(i))}$$

D'où $\theta(\sigma \circ \tau) = \theta(\sigma)\theta(\tau)$.

4. Montrons la question 4 : Soit G un groupe d'ordre 63. $63 = 7 \times 9 = 7 \times 3^2$. Par le premier théorème de Sylow, G admet un 7-Sylow. Par le deuxième théorème de Sylow, $n_7 \equiv 1 \pmod 7$ et $n_7 \mid 9$. Donc $n_7 \in \{1, 3, 9\}$. Or $9 \equiv 2 \pmod 7$ et $3 \equiv 3 \pmod 7$. Donc $n_7 = 1$. Donc il existe un unique 7-Sylow. Donc il est distingué dans G.

5. Montrons la question 5 : Soient $h, h' \in H$, $k, k' \in K$. Montrons que $g = hkh'k' \in HK$. Puisque H normalise K, il existe k'' tel que $kh' = h'k''$. Donc $g = hh'k''k' \in HK$. Le reste est clair. Démontrons maintenant la formule : On considère l'application

$$\varphi : H \times K \to HK, \ (h, k) \mapsto hk$$

L'application est clairement surjective, mais elle n'a pas d'intérêt à être injective. Regardons quand $hk = h'k'$. Alors $h'^{-1}h = k'k^{-1}$. D'où il existe $x \in H \cap K$ tel que $h = h'x$ et $k = x^{-1}k'$. On munit alors $H \times K$ de la relation d'équivalence :

$$(h, k) \sim (h', k') \iff \exists x \in H \cap K, \ h = h'x \text{ et } k = x^{-1}k'$$

Ainsi, puisque $|H \times K| = |H||K|$, et que chaque élément de HK est l'image d'exactement $|H \cap K|$ couples, on obtient la formule souhaitée.

Question 1. *Démontrer le théorème de Cayley, et que tout groupe de permutation s'injecte dans $GL_n(K)$ où K est un corps.*

Question 2. *A partir du premier théorème de Sylow, montrer que si $|G| = p^\alpha m$, alors pour tout $i \in [\![1, \alpha]\!]$, G admet un sous-groupe d'ordre p^i.*

Question 3. *A partir du deuxième théorème de Sylow, montrer que si S un p-Sylow de G, alors sont équivalents : $S \trianglelefteq G$ et S est l'unique p-Sylow de G.*

Question 4. *Montrer qu'un groupe d'ordre 63 n'est pas simple.*

Question 5. *Soient H, K deux sous groupes de G, tels que H normalise K. Alors HK est un sous-groupe de G, et :*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Recasages

Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

Leçon 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Leçon 104 : Groupes finis. Exemples et applications.

Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.