Développement : le premier théorème de Sylow

Léo Daures

Leçons 101, 103, 104, (106), (123)

Référence : Perrin

1 Premier théorème de Sylow

Dans la suite, p désigne un nombre premier et G un groupe fini d'ordre $n = p^\alpha m$, où $m \wedge p = 1$. (Éventuellement, $\alpha = 0$).

Définition 1. *Un $p-$Sylow de G est un sous-groupe de G d'ordre p^α. Autrement dit, c'est un $p-$sous-groupe de G d'ordre maximal.*

Théorème 1. *G admet un $p-$Sylow.*

Ce théorème est le premier des théorèmes de Sylow, qui donnent des propriétés de l'ensemble des $p-$Sylows d'un groupe G (qui est utile pour trouver des propriétés de G lui-même).

2 Démonstration

Commençons par observer un cas particulier, qui nous servira par la suite : le cas de $GL_d(\mathbb{Z}/p\mathbb{Z})$. Avant toute chose, rappelons son cardinal.

Lemme 1. $|GL_d(\mathbb{Z}/p\mathbb{Z})| = (p^d - 1)(p^d - p) \dots (p^d - p^{d-1})$.

Preuve. Calculer le cardinal de $GL_d(\mathbb{Z}/p\mathbb{Z})$ revient à compter les bases de $(\mathbb{Z}/p\mathbb{Z})^d$. En effet, $GL_d(\mathbb{Z}/p\mathbb{Z})$ est en bijection avec l'ensemble des bases de $(\mathbb{Z}/p\mathbb{Z})^d$ via $M \mapsto (Me_1, Me_2, \dots, Me_d)$ où $(e_1, \dots, e_d)$ est la base canonique de $(\mathbb{Z}/p\mathbb{Z})^d$.

Comment se définit une base de $(\mathbb{Z}/p\mathbb{Z})^d$? En choisissant l'un après l'autre les vecteurs qui la constituent. Prenons d'abord un premier vecteur non nul, ce qui laisse le choix entre $p^d - 1$ vecteurs. Après ce choix, il faut déterminer un deuxième vecteur de base. Celui-ci peut être choisi n'importe où dans $(\mathbb{Z}/p\mathbb{Z})^d$ sauf dans $\mathrm{Vect}\{e_1\}$, ce qui laisse $p^d - |\mathrm{Vect}\{e_1\}| = p^d - p$ possibilités. Le troisième vecteur de base doit ensuite être cherché dans $(\mathbb{Z}/p\mathbb{Z})^d \backslash \mathrm{Vect}\{e_1, e_2\}$, avec $p^d - p^2$ possibilités, et par un argument rapide de récurrence, le k-ème vecteur de base est choisi parmi $p^d - p^{k-1}$ possibilités. Ainsi, après le choix du d-ème vecteur on est assuré d'avoir déterminé une base, et on a eu le choix entre exactement $(p^d - 1)(p^d - p) \dots (p^d - p^{d-1})$ possibilités $\square$

Remarquons que $|GL_d(\mathbb{Z}/p\mathbb{Z})| = (p^d - 1)(p^d - p) \dots (p^d - p^{d-1}) = p^{d(d-1)/2} m$ avec $m = (p^d - 1)(p^{d-1} - 1) \dots (p - 1)$ (on a factorisé autant qu'on le pouvait chacun des facteurs $p^d - p^k$) et que $p \wedge m = 1$. On se retrouve bien dans la situation de l'énoncé du premier théorème de Sylow avec $\alpha = \frac{d(d-1)}{2}$. Si le théorème est bien vrai, on devrait pouvoir trouver un $p-$Sylow dans le groupe $GL_d(\mathbb{Z}/p\mathbb{Z})$. On en exhibe effectivement un avec le lemme suivant :

Lemme 2. *Le sous-groupe de $GL_d(\mathbb{Z}/p\mathbb{Z})$ constitué des matrices triangulaires supérieurs strictes (i.e. avec des 1 sur la diagonale) est d'ordre $p^{d(d-1)/2}$. Il est donc de fait un $p-$Sylow de $GL_d(\mathbb{Z}/p\mathbb{Z})$.*

preuve. Le fait qu'il s'agisse d'un sous-groupe découle des règles de calcul matriciel. Il faut maintenant de compter le nombre de matrices triangulaires supérieurs strictes de $\mathcal{M}_d(\mathbb{Z}/p\mathbb{Z})$ (elles sont toutes instantanément inversibles puisqu'elles n'ont que des 1 sur la diagonale). Ce calcul s'avère bien plus facile que le précédent : il suffit de choisir chacun des $d(d-1)/2$ coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Il y a donc exactement $p^{d(d-1)/2}$ possibilités ! □

On a trouvé un $p-$Sylow dans le groupe $GL_d(\mathbb{Z}/p\mathbb{Z})$. Ce cas particulier parait anodin, mais il est la clé pour trouver un $p-$Sylow de n'importe quel groupe fini ! On s'aidera pour cela du lemme suivant :

Lemme 3. *Soit G un groupe fini d'ordre $p^\alpha m$ (avec $p \wedge m = 1$) et H un sous-groupe de G d'ordre $p^\beta \ell$ (avec $p \wedge \ell = 1$). Si G admet un $p-$Sylow, alors H admet un $p-$Sylow (attention : ce sous-groupe n'est plus de cardinal p^α mais est bien un $p-$sous-groupe de H de cardinal maximal, c'est-à-dire de cardinal p^β).*

Alors, il suffit de voir G comme un sous-groupe d'un certain $GL_d(\mathbb{Z}/p\mathbb{Z})$ pour conclure ! Comment injecter G dans $GL_d(\mathbb{Z}/p\mathbb{Z})$? On peut pour commencer l'injecter dans $\mathfrak{S}_n$ grâce au théorème de Cayley. Par suite, $\mathfrak{S}_n$ peut être vu comme un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$, celui des matrices de permutations. Ainsi, G est un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$. Comme $GL_n(\mathbb{Z}/p\mathbb{Z})$ a un $p-$Sylow, G en a un aussi d'après le dernier lemme. La seule chose qu'il reste à faire est démontrer le lemme en question.

preuve du lemme 3. Notons S le $p-$Sylow de G donné par les hypothèses. On cherche à identifier des $p-$sous-groupes de H, parmi lesquels on espère trouver un $p-$Sylow de H. On en connaît au moins un : $S \cap H$ est un $p-$sous-groupe de H (c'est un sous-groupe de S donc son ordre divise p^α et c'est donc un $p-$groupe). Malheureusement, même s'il est un $p-$sous-groupe de H, rien ne dit que c'en soit un $p-$Sylow. Il va falloir observer d'autres $p-$sous-groupes de H. On peut heureusement en construire un certain nombre en conjugant S : aSa^{-1} est un $p-$sous-groupe de G, car il est en bijection avec S (un oeil averti remarquera même que c'est un $p-$Sylow de G, mais c'est l'objet du deuxième théorème de Sylow et cette remarque est inutile ici). Comme précédemment, $aSa^{-1} \cap H$ est donc un $p-$sous-groupe de H (c'est un sous-groupe de aSa^{-1} donc son ordre divise $|aSa^{-1}| = p^\alpha$, ce qui en fait un $p-$groupe). Maintenant qu'on dispose d'un certain nombre de $p-$sous-groupes de H, la démonstration repose sur l'idée de voir ces $p-$sous-groupes comme les stabilisateurs d'une action.

Considérons l'ensemble $G/S = \{aS, a \in G\}$ des classes à gauche de G. Ce n'est pas *a priori* un groupe, mais on sait que son cardinal $|G/S| = [G : S] = p^\alpha m / p^\alpha = m$ n'est pas multiple de p. G agit sur G/S par translation à gauche $g \cdot aS = (ga)S$. aSa^{-1} est alors le stabilisateur $\mathrm{Stab}_G(aS)$ de aS. En effet, $\forall s \in S, (asa^{-1}) \cdot aS = (asa^{-1}a)S = (as)S = aS$ et réciproquement :

$$g \cdot aS = aS \Rightarrow \forall s \in S, \exists s' \in S, gas = as' \Rightarrow g = as's^{-1}a^{-1} \in aSa^{-1}$$

Les sous-groupes de G ne nous intéressent pas, nous cherchons des sous-groupes de H. Il est donc naturel de considérer plutôt l'action par translation à gauche de H sur G/S. Il s'agit de la même action qu'avec G tout entier, mais on ne regarde que les éléments de H qui agissent sur G/S. Le stabilisateur de aS pour cette action est :

$$\mathrm{Stab}_H(aS) = \{g \in H, g \cdot aS = aS\} = \{g \in G, g \cdot aS = aS\} \cap H = \mathrm{Stab}_G(aS) \cap H = aSa^{-1} \cap H$$

On peut donc voir $aSa^{-1} \cap H$ comme un stabilisateur pour une action, et on va donc pouvoir utiliser les outils consacrés aux actions de groupes.

Nous cherchons maintenant à trouver un a tel que le $p-$sous-groupe $\mathrm{Stab}_H(aS)$ soit exactement d'ordre p^β. Par la relation orbite-stabilisateur (qui dit que $|\mathrm{Orb}_H(aS)| \times |\mathrm{Stab}_H(aS)| = |H| = p^\beta \ell$ pour tout $aS \in G/S$), cela revient à trouver un a tel que $|\mathrm{Orb}_H(aS)| \wedge p = 1$. Supposons par l'absurde que p divise le cardinal de chacune des orbites. Les orbites forment une partition de G/S, donc le cardinal de G/S est la somme des cardinaux des orbites. Comme p divise chacun des termes de la somme, il divise $|G/S|$ ... mais c'est absurde car d'après une remarque précédente, $|G/S| = m$, donc $|G/S| \wedge p = 1$! Donc il existe un $a \in G$ tel que $|\mathrm{Orb}_H(aS)| \wedge p = 1$ *i.e.* $|aSa^{-1} \cap H| = p^\beta$, et $aSa^{-1} \cap H$ est un $p-$Sylow de H !

On a même dans cette preuve affiné le lemme. Non seulement on a trouvé un $p-$Sylow de H, mais on a aussi trouvé une forme agréable sous laquelle rechercher un $p-$Sylow de H, à savoir un $aSa^{-1} \cap H$. □