Développement: Théorème de Sylow

Adrien Fontaine

19 janvier 2013

Référence : Perrin, p19-20

Théorème 1

Soit G un groupe fini, de cardinal $|G| = p^\alpha m$ avec $p \nmid m$. Alors :

1. *Il existe un p-sous groupe de Sylow de G.*
2. *Tous les p-Sylow de G sont conjugués entre eux.*
3. *Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$.*

Pour prouver ce théorème, on a d'abord besoin d'un lemme.

Lemme 1

Soit G un groupe de cardinal $|G| = p^\alpha m$ avec $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Démonstration : Le groupe G opère sur G/S par translation à gauche :

$$\begin{array}{ccc} G \times G/S & \to & G/S \\ (g, aS) & \mapsto & g.(aS) = (ga)S \end{array}$$

Il est alors facile de voir que le stabilisateur de aS est le sous-groupe aSa^{-1}, conjugué de S. (S n'est pas forcément distingué, donc G/S n'est pas nécessairement un groupe. Cela désigne simplement l'ensemble des classes à gauche modulo S.)
Mais H opère lui aussi sur G/S par restriction, avec comme stabilisateur de aS, $aSa^{-1} \cap H$.
Il reste à voir que l'un de ces groupes est un Sylow de H. Or, S est un p-Sylow donc aSa^{-1} aussi, donc les $aSa^{-1} \cap H$ sont des p-groupes.
Il suffit donc de montrer qu'il existe $a \in G$ tel que $|H/(aSa^{-1} \cap H)|$ soit premier à p (on a $|H| = p^\beta n$ avec $\beta \leq \alpha$ et $p \nmid n$, et $|aSa^{-1} \cap H|$ est une puissance de p).
Par ailleurs, l'application

$$\begin{array}{ccc} H/(aSa^{-1} \cap H) & \to & \omega(aS) \\ \bar{g} & \mapsto & g.aS \end{array}$$

(où $\omega(aS)$ désigne l'orbite de aS sous l'action de H sur G/S) est une bijection (on quotiente par la relation d'équivalence,

$$\begin{aligned} g \sim g' &\Leftrightarrow g.aS = g'.aS \\ &\Leftrightarrow (gg'^{-1}).aS = aS \\ &\Leftrightarrow gg'^{-1} \in Stab(aS) \\ &\Leftrightarrow gg'^{-1} \in aSa^{-1} \cap H \end{aligned}$$

) Donc, $|H/(aSa^{-1} \cap H)| = |\omega(aS)|$. Si tous ces nombres étaient divisibles par p, il en serait de même de $|G/S|$, car G/S est réunion des orbites $\omega(aS)$. Mais ceci contredit le fait que S est un p-Sylow de G. ■

Passons maintenant à la preuve du théorème de Sylow.

Démonstration du théorème de Sylow : 1. D'après le théorème de Cayley (si G est fini, et de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$), on peut plonger G dans $\mathfrak{S}_n$. On peut ensuite plonger $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ via :

$$\begin{array}{ccccccc} \mathfrak{S}_n & \to & GL_n(\mathbb{F}_p) & & & & \\ \sigma & \mapsto & u_\sigma & : & e_i & \mapsto & e_{\sigma(i)} \end{array}$$

(où (e_i) est la base canonique de $\mathbb{F}_p^n$). Finalement, on a donc réalisé G comme un sous-groupe de $GL_n(\mathbb{F}_p)$.
Or,

$$\begin{aligned} |GL_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p)...(p^n - p^{n-1}) \\ &= p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1)...(p - 1) \\ &= mp^{n(n-1)/2} \text{ avec } p \nmid m \end{aligned}$$

On exhibe alors aisément un p-sous groupe de Sylow de $GL_n(\mathbb{F}_p)$:

$$P = \{A = (a_{i,j}) / a_{i,j} = 0 \text{ pour } i > j \text{ et } a_{i,i} = 1\}$$

On peut donc voir G comme un sous-groupe de $GL_n(\mathbb{F}_p)$, qui possède un p-Sylow, donc G aussi d'après le lemme précédent.

2. On prouve en fait 2. et 3. simultanément. Si H est un p-sous-groupe et S un p-Sylow de G, il existe d'après le lemme, $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, on a $aSa^{-1} \cap H = H$. Donc, H est inclus dans aSa^{-1} qui est un p-Sylow. Si de plus, H est un p-Sylow, on a exactement $H = aSa^{-1}$. ■