Sandrine CARUSO

Théorème de Sylow.

Référence : Perrin

Théorème (Sylow). *Soit G un groupe de cardinal $n = p^\alpha m$, où p est premier, et m n'est pas divisible par p.*

1. *Tout p-sous-groupe de G est inclus dans un p-groupe de Sylow de G.*
2. *Les p-groupes de Sylow de G sont conjugués (en particulier, le nombre n_p de p-groupes de Sylow divise n).*
3. *$n_p \equiv 1 \pmod p$.*

Lemme. *Soit S un p-groupe de Sylow de G, et H un sous-groupe de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-groupe de Sylow de H.*

Démonstration. Le groupe H opère naturellement sur les classes à gauche G/S, par translation à gauche : $h \cdot aS = haS$. Le stabilisateur d'un élément a par cette action est

$$\mathrm{Stab}(aS) = \{h \in H, haS = aS\} = \{h \in H, a^{-1}ha \in S\} = aSa^{-1} \cap H.$$

Il suffit de montrer qu'il existe $a \in G$ tel que $\frac{\# H}{\#(aSa^{-1} \cap H)}$ soit premier avec p. D'après la formule des classes,

$$\frac{\# H}{\#(aSa^{-1} \cap H)} = \#(\mathrm{Orb}(aS)).$$

Supposons que pour tout $a \in G$, $\#(\mathrm{Orb}(aS))$ soit divisible par p. Mais alors $\# G/S = \frac{\# G}{\# S}$ est également divisible par p car G/S est réunion disjointe des orbites, et cela contredit le fait que S est un p-groupe de Sylow de G.

On en déduit qu'il existe a tel que $\#(\mathrm{Orb}(aS))$ ne soit pas divisible par p, et ainsi $aSa^{-1} \cap H$ est un p-groupe de Sylow de H. $\square$

Soit H un p-sous-groupe de G et S un p-Sylow de G. D'après le lemme, il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H. Mais comme H est lui-même un p-groupe, nécessairement $H = aSa^{-1} \cap H$, ce qui montre que $H \subset aSa^{-1}$ qui est un p-Sylow de G, d'où le point 1 du théorème. Le point 2 s'obtient en remarquant que dans le cas où H est un p-Sylow, ce qui précède donne $H = aSa^{-1}$.

Établissons maintenant le point 3. Soit encore S un p-Sylow de G. Notons X l'ensemble des p-Sylow de G. D'après le point 2, S agit sur X par conjugaison : si $s \in S$ et $T \in X$, $s \cdot T = sTs^{-1}$. On note $X^S = \{T \in X, \forall s \in S, s \cdot T = T\}$ l'ensemble des points fixes par cette action. L'ensemble X est la réunion des orbites sous l'action de

S, orbites dont le cardinal divise $\# S$, donc divise p^α. Ainsi, le cardinal d'une orbite est soit égal à 1, soit divisible par p, ce qui implique que

$$\# X \equiv \#(X^S) \pmod p.$$

Montrons que $\#(X^S) = 1$. On a déjà $S \in X^S$. Soit $T \in X^S$, et notons N le sous-groupe de G engendré par S et T. Les groupes S et T sont bien sûr encore des p-Sylow de N. Nous allons établir que T est distingué dans N. En effet, si $g \in N$, on peut écrire $g = s_1 t_1 \cdots s_r t_r$ avec $s_i \in S$ et $t_i \in T$. Si, maintenant, $t \in T$, on a

$$gtg^{-1} = s_1 t_1 \cdots s_r t_r t t_r^{-1} s_r^{-1} \cdots t_1^{-1} s_1^{-1}.$$

Comme, pour tout $s \in S$, $sTs^{-1} = T$, par récurrence, l'élément ci-dessus est bien un élément de T, donc $T \lhd N$. Or, d'après le point 2 appliqué au groupe N, T et S sont conjugués dans N. On en déduit que $T = S$.