Théorèmes de Sylow

En général, pour un groupe fini G et un entier positif n divisant l'ordre de G, il n'existe pas forcement un sous-groupe de G d'ordre n. Par exemple, le groupe alterné A_4 n'a pas de sous-groupe d'ordre 6, et $6 \mid 12 = |A_4|$. Mais, si on considère des puissances de premiers divisant l'ordre de G, alors il y a toujours un sous-groupe de G de cet ordre.
Des propriétés cruciales des sous-groupes d'ordre une puissance de premier seront présentés dans cette section. On commence par quelques définitions:

Définition

Soit p un nombre premier. On dit que H est un p-groupe si $|H| = p^\alpha$ pour α un entier positif.

Remarque Le groupe triviale est un p-groupe pour tout premier p, et c'est le seul groupe avec cette propriété.

Définition

Soit G un groupe fini et p un nombre premier. Supposons que $|G| = p^\alpha \cdot m$ avec $(p, m) = 1$.
On dit que H est un p-sous-groupe de G si H est un sous-groupe de G et un p-groupe.
On dit que H est un p-sous-groupe de Sylow si $|H| = p^\alpha$
Autrement dit, H est un p-sous-groupe de G d'ordre maximal.
On dénote par $Syl_p(G)$ l'ensemble de p-sous-groupes de Sylow de G et par n_p la cardinalité de $Syl_p(G)$.

Théorème (Sylow).

Soit G un groupe fini et p un nombre premier. Alors

1) Il existe un p-sous-groupe de Sylow de G
2) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.
3) Les p-sous-groupes de Sylow sont conjugués par des éléments de G.
4) On a les propriétés suivantes des $n_p = |Syl_p(G)|$
$n_p \mid m$ où $|G| = p^\alpha \cdot m$, avec $(p, m) = 1$; $n_p \equiv 1 \pmod p$.

Preuve. On suppose que $p \mid |G|$, sinon 1 est un p-sous-groupe de Sylow.

1) On raisonne par induction sur $|G|$. Si G a un sous-groupe H d'indice différent de 1 et premier à p, alors, par induction H possède un p-sous-groupe de Sylow, qui est aussi un p-sous-groupe de Sylow de G.

Donc on peut supposer que tous les sous-groupes propres de G sont d'indice dans G divisible par p. On considère l'équation des classes de G :

$$|G| = |Z(G)| + \sum_{x \in S''} |G : G_x|$$

où S'' est l'ensemble des représentants dans G d'orbites non-triviales et G_x est le sous-groupe d'isotropie de x. Par la supposition du paragraphe précédant, $|G : G_x|$ est divisible par p, pour tout $x \in S''$. Comme $p \mid |G|$, il s'en suit que $p \mid |Z(G)|$. En particulier, $Z(G)$ est non-trivial. Soit $y \in Z(G)$ un élément d'ordre p. Alors $\langle y \rangle \simeq C_p$ est un sous-groupe normal de G (même central) et $|G/\langle y \rangle| = \frac{|G|}{p} < |G|$. Ainsi, par induction $G/\langle y \rangle$

possède un sous-groupe de Sylow d'ordre $p^{\alpha-1}$, où $|G| = p^\alpha \cdot m$, $(m,p)=1$. Soit H l'image inverse de ce sous-groupe de Sylow sous la projection canonique $G \longrightarrow G/\langle y\rangle$. On a que $|H| = p^{\alpha-1}\cdot p = p^\alpha$ donc H est un p-sous-groupe de Sylow de G.

2) Soit H un p-sous-groupe de Sylow de G et $\mathcal{X} := \{gHg^{-1} \mid g \in G\}$ la classe de conjugaison de H dans G. Le groupe G agit transitivement sur $\mathcal{X}$. On a donc $|\mathcal{X}| = |G : G_H|$, où G_H est le normalisateur de H dans G. En particulier, $H \leq G_H$, donc $|G:G_H| \mid m$. Comme $(p,m)=1$, il s'en suit que $|\mathcal{X}|$ n'est pas divisible par p.

Soit $K \neq 1$ un p-sous-groupe quelconque de G. On fait K agir sur $\mathcal{X}$. On a :

$$|\mathcal{X}| = |\mathrm{Fix}(\mathcal{X})| + \sum_{x \in S''} |K : K_x|$$

Comme chacque terme de la somme est divisible par p et $|\mathcal{X}|$ ne l'est pas, il s'en suit que $\mathrm{Fix}(\mathcal{X}) \neq 0$. Donc, il existe $g \in G$, tel que, pour tout $k \in K$, $k(gHg^{-1})k^{-1} = gHg^{-1}$. Autrement dit, K normalise $H' := gHg^{-1}$. Mais alors $H'K$ est un sous-groupe de G et $|H'K| = \frac{|H'||K|}{|H' \cap K|}$. Donc $H'K$ est un p-groupe. De plus $|H'| = |gHg^{-1}| = |H| = p^\alpha$ donc H' est un p-sous-groupe de G maximal. il s'en suit que $KH' = H'$, ce qui implique $K \leq H'$. Ceci démontre 2)

3) En prenant K un p-sous groupe de Sylow de G et

en suivant la preuve de 2), on obtient que il existe $g \in G$, tel que $K \leq gHg^{-1}$. Comme K est aussi maximal, on obtient $K = gHg^{-1}$. Donc tout sous-groupe de Sylow de G est le conjugué d'un sous-groupe de Sylow donné H. Par transitivité, on obtient 3).

4) Dans la preuve de 2) nous avons obtenu que $n'_p := |\mathcal{H}| / m$. Par 3) on a que $\mathcal{H} = Syl_p(G)$, donc $n_p = n'_p$. Pour obtenir la congruence modulo p, on fait agir H sur $Syl_p(G)$ par conjugaison. Mais, comme dans 3), si K est normalisé par H, alors $H = K$. Donc le seul point de $Syl_p(G)$ fixé par l'action de H est H. Les autres orbites sont de longueur divisible par p. Donc :

$$n_p = |Syl_p(G)| \equiv 1 \pmod{p}.$$