P. Maurer

ENS Rennes

Recasages : 101, 103, 104.

Référence : Perrin, Algèbre & Serre, Groupes finis.

Théorèmes de Sylow

Version de Wielandt

Lemme 1. *Soit p un nombre premier, $r \in \mathbb{N}$ et $m \leq n$. On a la congruence :*

$$\begin{pmatrix} p^r n \\ p^r m \end{pmatrix} \equiv \begin{pmatrix} n \\ m \end{pmatrix} \pmod{p}$$

Démonstration. Dans l'anneau $\mathbb{F}_p[X]$, on a les égalités :

$$\begin{aligned} \sum_{\ell=0}^{p^r n} \begin{pmatrix} p^r n \\ \ell \end{pmatrix} X^\ell &= (X+1)^{p^r n} \\ &= (X^{p^r}+1)^n \\ &= \sum_{\ell=0}^{n} \begin{pmatrix} n \\ \ell \end{pmatrix} X^{p^r \ell} \end{aligned}$$

En identifiant les coefficients des monômes de degré $p^r \ell$, on obtient le résultat souhaité. □

Théorème 2. *Soit G un groupe fini d'ordre $n = p^\alpha m$ avec $p \nmid m$. Alors :*

i. G admet un p-Sylow.

ii. Les p-Sylow de G sont conjugués entre eux.

iii. En notant k le nombre de p-Sylow, on a $k \equiv 1[p]$ et $k|m$.

Démonstration.

i. On considère l'ensemble X des parties de G de cardinal p^α et l'ensemble Y des p-Sylows de G.

On fait opérer G sur X par translation à gauche. Soit $E \in X$, et G_E le stabilisateur de E pour cette action. Pour tout $g \in G_E$, on a $gE = E$ donc à $t \in E$ fixé, l'application $\varphi_t : g \in G_E \mapsto gt$ est à valeurs dans E, et elle est injective car si $gt = ht$, on a $h^{-1}gt = t$ et comme $t \in G$, t est inversible donc $h = g$. On en déduit que $|G_E| \leq p^\alpha$.

Montrons qu'on a de plus $|G_E| = p^\alpha \iff E = Sx$ avec $x \in G$ et $S \in Y$, et que dans ce cas, $G_E = S$.

$\boxed{\Longrightarrow}$ Supposons que G_E ait p^α éléments. Comme c'est un sous-groupe de G, c'est donc un p-Sylow, donc $G_E \in Y$. De plus, pour $t \in E$, l'application φ_t définie précédemment est alors une bijection, donc pour tout $g \in G_E$, il existe un unique $h \in G_E$ tel que $ht = g$: on a donc $G_E \subset G_E t$, et l'inclusion réciproque est claire.

$\boxed{\Longleftarrow}$ Réciproquement, le stabilisateur de Sx pour $S \in Y$ et $x \in G$ est S, en particulier on a $|G_{S_x}| = p^\alpha$.

On considère alors l'équation aux classes :

$$|X| = \sum_{E \in X} \frac{|G|}{|G_E|} = \left(\sum_{\substack{E \in X \\ |G_E| = p^\alpha}} \frac{|G|}{|S|} + \sum_{\substack{E \in X \\ |G_E| < p^\alpha}} \frac{|G|}{|G_E|} \right) \equiv |Y| m \pmod{p} \quad (\star)$$

Déterminons le cardinal de X directement, via l'utilisation du **Lemme 1** [(1)] :

$$\begin{aligned} |X| &= |\{H \subset G : |H| = p^\alpha\}| \\ &= \binom{p^\alpha m}{p^\alpha} \\ &\equiv \binom{m}{1} \pmod{p} \\ &\equiv m \pmod{p} \end{aligned}$$

Via $(\star)$, on a donc l'identité $m \equiv |Y| m \pmod{p}$, i.e :

$$p \mid m(|Y| - 1)$$

Comme p est premier avec m, il vient que $|Y| \equiv 1 \pmod{p}$, ce qui prouve l'existence d'un p-Sylow (en tant qu'élément de $Y \neq \varnothing$), ainsi que la congruence de iii.

ii. Soit $S \in Y$ et H un p-sous-groupe de G. H opère sur le quotient $G/S = \{gS : g \in G\}$ de S sous G.

On applique la formule des classes, et il vient :

$$|G/S| = \sum_{\mathrm{Orb}(gS)} \frac{|H|}{|\mathrm{Stab}(gS)|}$$

Comme $|G/S| = m$ et $p \nmid m$, il existe $g \in G$ tel que $|\mathrm{Stab}(gS)| = |H|$. On a donc, pour ce g donné, $HgS = gS$, donc $H \subset gSg^{-1}$. Si H est de plus un p-Sylow, l'égalité des cardinaux donne $H = gSg^{-1}$, i.e les Sylow sont conjugués entre eux.

iii. D'après ce qui précède, G agit transitivement par conjugaison sur l'ensemble des p-Sylow Y, donc l'équation aux classes s'écrit simplement $|Y| = |G|/|\mathrm{Stab}(S)|$ où $S \in Y$. En particulier, $|Y|$ doit diviser $|G|$, donc puisque $|Y| \equiv 1 \,(\mathrm{mod}\, p)$, $|Y|$ divise m, ce qui conclut la preuve. □

[(1)] : Il est possible de se passer du **Lemme 1** en appliquant ce qui précède à $\mathbb{Z}/n\mathbb{Z}$ avec $n = p^\alpha m$. En effet, le groupe $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre d pour d divisant n, en particulier, il admet un unique p-Sylow, donc on a $|Y| = 1$, donc $|X| \equiv m\,[p]$ dans $\mathbb{Z}/n\mathbb{Z}$ d'après $(\star)$. On remarque alors que $|X|$ ne dépend que du cardinal du groupe et non pas de sa structure, donc l'égalité $|X| \equiv m[p]$ reste valable dans n'importe quel groupe d'ordre $p^\alpha m$.