Une preuve combinatoire du théorème de Wilson.

par Bruno Deschamps

Professeur à l'Université du Maine

RÉSUMÉ.— Nous donnons dans ce texte une preuve inattendue du théorème de Wilson utilisant le théorème de Sylow.

Un très célèbre théorème de John Wilson daté de 1759 affirme que si p est un nombre premier alors il y a la congruence suivante[1] :

$$(p-1)! \equiv -1 \bmod(p)$$

Les preuves classiques de ce théorème sont simples et restent abordables avec un matériel élémentaire de mathématique. En préparant un examen de théorie des groupes pour mes étudiants de licence je suis tombé presque malgré moi sur une preuve de ce résultat utilisant la théorie de Sylow. Ne l'ayant jamais vu écrite et la trouvant assez inattendue, je me propose de vous la présenter ici.

Commençons par faire quelques rappels de théorie de Sylow afin de rendre plus compréhensible l'approche au lecteur non aguerri à la théorie des groupes : étant donné un groupe G et un nombre premier p on appelle p-sous-groupe de G tout sous-groupe d'ordre une puissance de p. Un p-sous-groupe de Sylow de G est alors un p-sous-groupe maximal. La théorie de Sylow de base consiste en les deux théorèmes suivants :

Théorème 1.— (dit premier théorème de Sylow) *Soit G un groupe d'ordre $p^n s$ avec p premier, $n \geq 1$ et $(s,p) = 1$. Pour tout entier $r \in \{1, \cdots, n\}$ il existe un p-sous-groupe de G d'ordre p^r.*

Théorème 2.— (dit deuxième théorème de Sylow) *Soit G un groupe d'ordre divisible par le nombre premier p.*

a) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.

b) Les p-sous-groupe de Sylow de G sont conjugués.

c) Le nombre des p-sous-groupe sde Sylow de G est congru à 1 modulo p et divise l'ordre de G.

On remarquera que ces deux théorèmes impliquent, avec les notations du premier, que les p-sous-groupes de Sylow sont exactement les p-sous-groupes de G d'ordre p^n (certains auteurs prennent d'ailleurs cette propriété comme définition). Sur ce sujet, nous renvoyons le lecteur à l'excellent ouvrage de Josette Calais "Eléments de théorie des groupes" publié aux PUF où sont

[1] Ce résultat était en fait déjà connu de Leibniz qui ne l'avait pas publié

présentées les bases de la théorie élémentaire des groupes et en particulier les théorèmes de Sylow.

On considère donc un nombre premier p et S_p le p-ième groupe symétrique. La preuve dont il est question s'obtient en dénombrant les p-sous-groupes de Sylow de S_p. On y arrive en remarquant les deux propriétés suivantes :

Lemme 1.— *Dans S_p les éléments d'ordre p sont exactement les p-cycles. En particulier, il y a exactement $(p-1)!$ éléments d'ordre p dans S_p.*

Preuve : Les p-cycles sont bien sur des éléments d'ordre p dans S_p (cette propriété étant indépendante du fait que p soit premier). Soit maintenant une permutation $\sigma \in S_p$ d'ordre p et

$$\sigma = \gamma_1 \circ \cdots \circ \gamma_n$$

sa décomposition canonique en produit de cycles disjoints. On sait que l'ordre $o(\sigma)$ de σ est égal au $\text{ppcm}(o(\gamma_1), \cdots, o(\gamma_n))$. Comme p est premier on en déduit que pour tout $i = 1, \cdots, n$ on a $o(\gamma_i) = p$ (le cas $o(\gamma_i) = 1$ est impossible car alors γ_i serait l'identité ce qui est exclu). Par ailleurs, puisque les cycles γ_i sont de supports disjoints de longueur p, on a obligatoirement $n = 1$ et donc $\sigma = \gamma_1$ est bien un p-cycle.

On peut écrire tout p-cycle de S_p sous la forme $(p\ s(1)\ \cdots\ s(p-1))$ (avec $s \in S_{p-1}$) et cette description étant visiblement biunivoque, on en déduit qu'il y en a donc exactement $(p-1)!$.

Lemme 2.— *Dans S_p les p-sous-groupes de Sylow sont exactement les sous-groupes d'ordre p (ils sont donc tous cycliques). En particulier le nombre de p-sous-groupes de Sylow dans S_p vaut $n_p = (p-2)!$.*

Preuve : Comme p est premier, la valuation p-adique de $p!$ vaut 1 (i.e. $p! = pm$ avec $m \in \mathbb{N}$ premier à p). On en déduit que les p-sous-groupes de Sylow de S_p sont les sous-groupes d'ordre p (ils sont donc tous cycliques isomorphes à $\mathbb{Z}/p\mathbb{Z}$).

Maintenant tout élément d'ordre p de S_p vit dans un p-sous-groupe de Sylow. Réciproquement, comme p est premier et qu'un p-sous-groupe de Sylow de S_p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il existe exactement $p-1$ éléments d'ordre p dans chaque p-sous-groupe de Sylow de S_p (puisque dans $\mathbb{Z}/p\mathbb{Z}$ tous les éléments non nuls sont générateurs). Ainsi, il y a $n_p = \dfrac{(p-1)!}{p-1} = (p-2)!$ p-sous-groupes de Sylow dans S_p.

Preuve du théorème de Wilson : le théorème de Sylow affirme en particulier que $n_p \equiv 1 \bmod(p)$, on a donc $(p-2)! \equiv 1 \bmod(p)$ ce qui donne, en multipliant par $(p-1)$, que $(p-1)! \equiv -1 \bmod(p)$.