Zeitschrift: L'Enseignement Mathématique

Band: 35 (1989)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LE THÉORÈME DE BURNSIDE SUR LE COMPTAGE DES ORBITES ET QUELQUES APPLICATIONS

Kapitel: 4. L'indicateur des cycles

Autor: Sigrist, François

DOI: https://doi.org/10.5169/seals-57367

Lemme 3.3. *Si* G *est résoluble,* S *en est l'unique sous-groupe d'ordre* p.

Preuve. G contient alors un sous-groupe dérivé $G^{(k)}$, non trivial et commutatif. Celui-ci contient donc un unique sous-groupe S' d'ordre p, par le corollaire du lemme 3.1. De ce fait, S' est normal dans G, et unique puisque d'indice premier à p. Par conséquent $S = S'$.

Remarque. Voici le passage correspondant de la démonstration de Galois dans le mémoire cité (le groupe G de ce texte est bien sûr S):

> ... donc le groupe qui précède immédiatement le groupe G ne devra contenir que des substitutions telles que x_k, x_{ak+b} et ne contiendra pas, par conséquent, d'autre substitution circulaire que celle du groupe G.
> On raisonnera sur ce groupe comme sur le précédent, et il s'ensuivra que le premier groupe dans l'ordre des décompositions, c'est-à-dire le groupe ACTUEL de l'équation ne peut contenir que des substitutions de la forme x_k, x_{ak+b}.

Lemme 3.4. *Si* S *est normal dans* G, G *est résoluble.*

Preuve. En numérotant convenablement les racines, on peut supposer que S est le sous-groupe T des translations du lemme 3.2. G est alors contenu dans le groupe A des affinités. C.Q.F.D.

Le chaînon manquant de la démonstration proprement dite est alors fourni par le théorème de Burnside. Grâce aux lemmes ci-dessus, il ne reste en effet qu'à invoquer la proposition 2.3: Si G agit de façon affine sur l'ensemble des racines, il ne peut contenir que $p - 1$ éléments d'ordre p, puisque ceux-ci sont sans point fixe. Le sous-groupe S est donc unique, et la preuve est complète.

Les équations de degré premier, solubles par radicaux, sont obligatoirement métacycliques par le corollaire du lemme 3.2. Dans la deuxième édition du livre de van der Waerden [8], le § 60 leur est consacré sous ce titre, reprenant l'argumentation de Galois. Dommage qu'il ne figure plus dans les éditions ultérieures.

4. L'indicateur des cycles

Une permutation de m objets est dite de type $(j_1, j_2, ..., j_m)$ si sa décomposition en cycles disjoints comprend j_1 points fixes, j_2 transpositions, ..., et j_m m-cycles. On parle de même du type de l'élément $g \in G$, lorsque G agit sur un ensemble E à m objets. La fonction génératrice des types, introduite par Pòlya [6], s'appelle *indicateur des cycles*:

$$Z(G\,;z_1, z_2, \ldots, z_m) = \frac{1}{|\,G\,|} \Sigma z_1^{j_1} z_2^{j_2} \ldots z_m^{j_m}\,.$$

En l'absence d'une référence à un ensemble sur lequel G agit, on convient de considérer la représentation régulière du groupe G. Il faut remarquer que même dans ce cas, l'indicateur des cycles ne caractérise pas le groupe: prendre par exemple deux groupes non isomorphes d'ordre p^3 et d'exposant p premier impair [1, chapitre VIII].

L'indicateur des cycles pour le groupe des permutations de m objets Σ_m est connu sous forme implicite: c'est le coefficient de t^m dans le développement en série de la fonction $\exp\big(\Sigma(z_i t^i/i)\big)$. En particulier:

$$Z(\Sigma_3\,; z_1, z_2, z_3) = \frac{1}{6}(z_1^3 + 3z_1z_2 + 2z_3)\,.$$

Dans de nombreux problèmes d'énumération (frises, colliers, etc.), c'est l'action du groupe cyclique C_m et du groupe diédral D_m sur les m sommets d'un polygone régulier qui intervient. Les indicateurs des cycles sont dans ces cas donnés par:

$$Z(C_m\,; z_1, z_2, \ldots, z_m) = \frac{1}{m} \sum_{d|m} \varphi(d)\, z_d^{m/d}$$

$$Z(D_{2s}\,; z_1, z_2, \ldots, z_{2s}) = \frac{1}{4s} \sum_{d|2s} \varphi(d)\, z_d^{2s/d} + \frac{s}{2} z_1^2 z_2^{s-1} + \frac{s}{2} z_2^s$$

$$Z(D_{2s+1}: z_1, z_2, \ldots, z_{2s+1}) = \frac{1}{4s+2} \sum_{d|2s+1} \varphi(d)\, z_d^{(2s+1)/d} + s z_1 z_2^s$$

Le théorème de Burnside peut s'exprimer à l'aide de l'indicateur des cycles, puisque le nombre de points fixes d'un élément g est égal à j_1. Pour trouver le nombre d'orbites, il suffit en effet de calculer la dérivée partielle $\partial Z/\partial z_1$ au point $z_1 = z_2 = \ldots = z_m = 1$.

5. Le théorème d'énumération de Pòlya

Dans l'article [6] intitulé « Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen », Pòlya décrit une méthode de dénombrement pour les configurations inéquivalentes par l'action d'un groupe de symétries. Conçu au départ pour compter les isomères d'une substance chimique de géométrie donnée, le procédé permet également de