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

Autor(en): **Sigrist, François**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **35 (1989)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-57367

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 35 (1989), p. 99-106

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

par François SIGRIST

1. INTRODUCTION

Le nombre d'orbites de l'action d'un groupe fini sur un ensemble fini est donné par la moyenne du nombre de points fixes, calculée sur le groupe. Dans le cas d'une action transitive, ce résultat est dû à Frobenius [3, p. 287]. Le cas général, assorti d'un perfectionnement intéressant, se trouve dans le livre de Burnside [1, chapitre X, théorème VII, p. 191]:

> "The sum of the numbers of symbols left unchanged by each of the permutations of a permutation group of order N is tN, where t is the number of transitive sets in which the group permutes the symbols. The sum of the squares of the numbers of symbols left unchanged by each of the permutations of a transitive group of order N is sN, where s is the number of transitive sets in which a subgroup leaving one symbol unchanged permutes the symbols."

L'application la plus connue de ce résultat se trouve dans un article de Pòlya paru en 1937 [6]. Je présenterai ci-après les principaux aspects de cette « Pòlya's theory of counting », une méthode très efficace de dénombrement. Mais au préalable, je montrerai comment le théorème de Galois sur les équations de degré premier peut servir d'illustration au théorème de Burnside. Je donnerai les démonstrations complètes pour les deux théorèmes, car on ne les trouve pas souvent dans les ouvrages d'enseignement ou dans les cours. Pour ne pas alourdir inutilement les énoncés, je supposerai toujours que l'action d'un groupe est *effective*, et donc que seule l'identité agit trivialement.

2. DÉMONSTRATION DU THÉORÈME DE BURNSIDE

Le groupe G, d'ordre N, agit sur l'ensemble E, à m éléments. On note o_i la cardinalité des orbites $O_i (i=1..t)$. G_x est le stabilisateur de $x \in E$, n_i est l'ordre de G_x pour $x \in O_i$, $\mathrm{Fix}(g)$ est l'ensemble des points fixes de $g \in G$, et a_i est le nombre d'éléments de G ayant exactement i points fixes.

PROPOSITION 2.1. $\Sigma \mid \mathrm{Fix}(g) \mid = tN$, *ou, de façon équivalente,* $\Sigma i a_i = t \Sigma a_i$.

Démonstration. Considérons l'ensemble P des paires (g, x) telles que $gx = x$. P contient d'une part $\Sigma \mid \mathrm{Fix}(g) \mid$, et d'autre part $\Sigma \mid G_x \mid = \Sigma o_i n_i = tN$ paires, d'où l'assertion.

Pour la deuxième partie de l'énoncé de Burnside, on suppose que G agit transitivement, et que s est le nombre (commun) d'orbites des stabilisateurs.

PROPOSITION 2.2. $\Sigma i^2 a_i = s \Sigma a_i$.

Démonstration. Choisissons un stabilisateur G', et notons a'_i le nombre d'éléments de G' ayant exactement i points fixes. Alors $m a'_i = i a_i$, car un élément de G avec i points fixes appartient à i stabilisateurs. La proposition 2.1, appliquée à G', donne $\Sigma i a'_i = s \mid G' \mid = sN/m$, d'où $\Sigma i^2 a_i = sN$, comme annoncé.

On dira que le groupe G agit de façon *affine* si tout élément de G ayant deux points fixes est l'identité. Avec cette définition, la proposition 2.1 permet d'énoncer:

PROPOSITION 2.3. *On suppose que G agit transitivement sur un ensemble E à m éléments. Alors l'action de G est affine si et seulement si G contient exactement $m - 1$ éléments sans point fixe.*

Démonstration. Avec les notations ci-dessus, l'action est affine si et seulement si $a_2 = a_3 = \ldots = a_{m-1} = 0$. Comme $a_m = 1$, la proposition 2.1 pour $t = 0$ devient $a_0 = a_2 + 2a_3 + 3a_4 + \ldots + (m-2)a_{m-1} + m - 1$.

C.Q.F.D

3. UN THÉORÈME DE GALOIS

« Le Mémoire ci-joint est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux et une seule application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages. On trouvera ici une CONDITION générale à laquelle SATISFAIT TOUTE ÉQUATION SOLUBLE PAR RADICAUX, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre Analyse:

Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il FAUT et il SUFFIT que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles... »

[4, Mémoire sur les conditions de résolubilité des équations par radicaux, extrait de la préface du 16 janvier 1831].

Ce résultat concernant les équations à coefficients rationnels, et dont la démonstration se déroule entièrement dans le contexte, et le vocabulaire, de la théorie des groupes, illustre de façon convaincante la nouveauté et la force des idées introduites par Galois.

A une équation de degré premier p, irréductible, correspond un groupe *transitif* G de permutations des p racines. G est donc d'ordre divisible par p, et contient par conséquent un sous-groupe S cyclique d'ordre p (Galois cite Cauchy, qui venait de démontrer cette propriété). Les éléments non triviaux de S sont des p-cycles, et n'ont donc aucun point fixe.

Si les racines peuvent s'exprimer rationnellement à partir de deux quelconques d'entre elles, cela équivaut au fait que le groupe G agit de façon *affine* sur l'ensemble des racines. Le théorème de Galois prend alors la forme: *G est résoluble si et seulement s'il agit de façon affine sur l'ensemble des racines.*

Pour la démonstration, il est commode de prouver préalablement les lemmes qui suivent, qui ont d'ailleurs un intérêt en eux-mêmes.

LEMME 3.1. *Soit G agissant transitivement, et N un sous-groupe normal de G. Alors toutes les orbites de N ont la même cardinalité.*

Preuve. Soient Nx et Ny deux orbites. Par transitivité de l'action de G, $y = gx$. Comme $Ng = gN$, l'action de g fournit une bijection de Nx sur Ny.

C.Q.F.D.

COROLLAIRE. *Si $|E| = p$ premier, tout sous-groupe normal non trivial de G est d'ordre divisible par p, puisqu'il agit transitivement.*

LEMME 3.2. *Soit T le sous-groupe du groupe symétrique Σ_m, engendré par la translation $\tau(i) = i + 1 \pmod m$. Alors le normalisateur de T dans Σ_m est le groupe des affinités $A = \{\alpha \mid \alpha(i) = ai + b \pmod m, (a, m) = 1\}$. Le groupe A est résoluble, et son action est (évidemment) affine.*

Preuve. Soit $\gamma \in A$. Alors $\gamma\tau\gamma^{-1} = \tau^a$ avec $(a, m) = 1$. Posons $b = \gamma(0) = \tau^b(0)$; alors

$$\gamma(i) = \gamma\tau^i(0) = \gamma\tau^i\gamma^{-1}(b) = \tau^{ai}(b) = \tau^{ai+b}(0) = ai + b \pmod m .$$

Pour la résolubilité de A, il suffit de remarquer que le quotient A/T est le groupe commutatif des inversibles modulo m.

COROLLAIRE. *Si $m = p$ premier, le groupe A est métacyclique, d'ordre $p(p-1)$.*

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*:

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

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 $\exp(\Sigma(z_i t^i/i))$. En particulier:

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

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:

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

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

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

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 $z_1 = z_2 = ... = z_m = 1$.

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

donner des informations sur les symétries d'une molécule lorsque l'on en connaît le nombre de différents isomères.

La situation de départ est celle d'un groupe G agissant sur un ensemble à m éléments, qui eux-mêmes peuvent être coloriés à l'aide de n couleurs. On demande de déterminer le nombre de colorations de E, inéquivalentes par l'action du groupe G. La solution donnée par Pòlya s'obtient en appliquant convenablement le théorème de Burnside:

THÉORÈME 5.1. *Le nombre de colorations de l'ensemble E à n couleurs, inéquivalentes par l'action de G, est $Z(G; n, n, ..., n)$.*

Démonstration. En agissant sur E, le groupe G agit également sur l'ensemble des colorations de E à n couleurs, et c'est le nombre d'orbites de cette action qu'il faut déterminer. Par le théorème de Burnside, on est ramené à compter les colorations de E qui sont fixes par un élément donné g de G. Mais une coloration n'est invariante par g que si elle est constante sur les cycles de g. Il y a donc $n^{j_1+j_2+\dots+j_m}$ colorations fixes par g, et par conséquent $Z(G; n, n, ..., n)$ orbites. C.Q.F.D.

L'application la plus connue est celle du comptage des colliers différents pouvant être formés avec des perles de deux couleurs. La suite des premières valeurs obtenues, en fonction du nombre total de perles, est 2, 3, 4, 6, 8, 13, 18, 30, 46, 78, 126, 224 ... Elle sert souvent d'exemple résistant au traitement par les différences finies.

Une version plus générale, dans laquelle un deuxième groupe agit sur l'ensemble des couleurs, a été donnée par de Bruijn [2]. On en trouve une application intéressante dans [5]: le comptage des différents thèmes dodécaphoniques cycliques, inéquivalents par transposition musicale.

6. CLASSIFICATION DES COLORATIONS

Si le groupe G est trivial, il est bien connu que les n^m colorations de l'ensemble E à l'aide de n couleurs peuvent être triées selon les couleurs utilisées. Il suffit de développer $(x_1+x_2+\dots+x_n)^m$, puisque le coefficient multinomial $(m; i_1, i_2, ..., i_n)$ est le nombre de colorations nécessitant i_1 fois la couleur x_1, i_2 fois la couleur $x_2, ...,$ et i_n fois la couleur x_n. On dira que de telles colorations ont le poids $(i_1, i_2, ..., i_n)$.

Dans le cas général, on peut appliquer un raisonnement analogue à chaque terme de la formule de Burnside. On doit alors tenir compte du fait que les colorations sont constantes sur les cycles des éléments du groupe G.

Si $g \in G$ est de type $(j_1, j_2, ..., j_m)$, il faut développer, en lieu et place de $(x_1 + x_2 + ... + x_n)^m$, le polynôme

$$(x_1 + x_2 + ... + x_n)^{j_1} \cdot (x_1^2 + x_2^2 + ... + x_n^2)^{j_2} \cdot ... \cdot (x_1^m + x_2^m + ... + x_n^m)^{j_m} .$$

On obtient ainsi une version plus précise du théorème 5.1, qui remplace le nombre de colorations par leur fonction génératrice:

THÉORÈME 6.1. *Le nombre de colorations de poids* $(i_1, i_2, ..., i_n)$, *inéquivalentes par l'action de* G, *est le coefficient de* $x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$ *dans*

$$Z(G; (x_1 + x_2 + ... + x_n), (x_1^2 + x_2^2 + ... + x_n^2), ..., (x_1^m + x_2^m + ... + x_n^m)) .$$

Pour obtenir le théorème dans une version encore plus générale, il reste à introduire une fonction génératrice des couleurs $\chi(x_1, x_2, ..., x_n)$ quelconque, à la place de $(x_1 + x_2 + ... + x_n)$. De façon pertinente, Pòlya donne à une telle fonction le nom d'*inventaire des figures*. Le raisonnement avec la formule de Burnside est le même que précédemment, et il vient:

THÉORÈME 6.2. *Si l'on colorie les éléments de* E *à l'aide de l'inventaire des figures* $\chi(x_1, ..., x_n)$, *les colorations inéquivalentes par l'action de* G *sur* E *ont pour fonction génératrice*

$$Z(G; \chi(x_1, x_2, ..., x_n), \chi(x_1^2, x_2^2, ..., x_n^2), ..., \chi(x_1^m, x_2^m, ..., x_n^m)) .$$

A ce degré de généralité, le résultat est d'une souplesse d'utilisation inattendue, comme en témoigne l'exemple qui suit [6], repris en détail dans le livre de Pòlya-Tarjan-Woods [7].

On se propose de compter les *alcools aliphatiques*, qui sont des molécules d'hydrocarbures dans lesquelles la configuration des atomes de carbone est celle d'un arbre. La racine de l'arbre est le radical OH, et la valence du carbone exige que les ramifications soient de degré inférieur ou égal à 3. La figure 1 en donne un exemple.

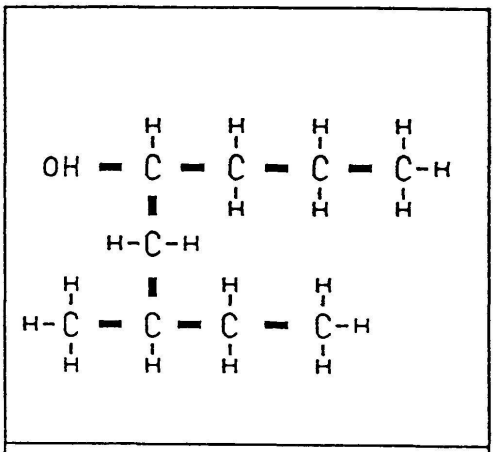

Figure 1

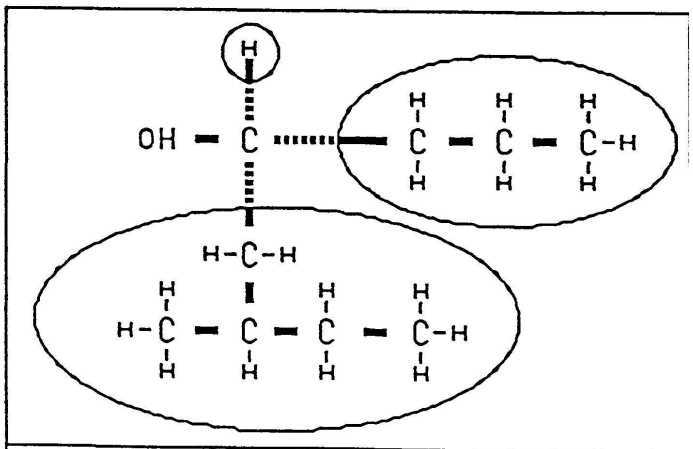

Figure 2

Il s'agit donc de trouver $a(n)$, le nombre d'arbres différents à n nœuds, avec toutes les ramifications de degré 1, 2 ou 3. On convient que $a(0) = 1$, et on note $A(x) = \Sigma a(n)x^n$ la fonction génératrice. On remarque alors qu'à tout arbre on peut en faire correspondre trois autres, qui sont les descendants de l'atome de carbone jouxtant la racine OH (voir Figure 2). Mais l'opération inverse, consistant à reconstruire un arbre à partir de trois autres, exige que l'on identifie les triplets d'arbres qui ne diffèrent que d'une permutation. On en déduit que la solution du problème est donnée par l'indicateur des cycles du groupe Σ_3, avec comme inventaire des figures la fonction $A(x)$ elle-même. Le théorème 6.2 devient ainsi, si l'on tient compte du nœud supplémentaire:

$$\frac{1}{x}\left(A(x)-1\right) = Z(\Sigma_3\,;\,A(x),\,A(x^2),\,A(x^3)) = \frac{1}{6}\left(A(x)^3+3A(x)A(x^2)+2A(x^3)\right).$$

Cette équation fonctionnelle pour la fonction $A(x)$ permet d'en trouver inductivement le développement en série, et les premiers termes sont

$$A(x) = 1 + x + x^2 + 2x^3 + 4x^4 + 8x^5 + 17x^6 + \ldots$$

RÉFÉRENCES

[1] BURNSIDE, W. *Theory of groups of finite order.* Second edition. Cambridge at the University Press (1911).

[2] DE BRUIJN, N. G. Color patterns that are invariant under a given permutation of the colors. *Journal of Combinatorial Theory 2* (1967), 418-421.

[3] FROBENIUS, G. Über die Kongruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmoduls. *Journal de Crelle 101* (1887), 277-293.

[4] GALOIS, E. *Œuvres mathématiques.* Gauthier-Villars (1897).

[5] GILBERT, E. N. and J. RIORDAN. Symmetry types of periodic sequences. *Illinois Journal of Mathematics 5* (1961), 657-665.

[6] PÒLYA, G. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen. *Acta Mathematica 68* (1937), 145-252.

[7] PÒLYA, G., R. TARJAN and D. WOODS. *Notes on Introductory Combinatorics.* Birkhäuser-Verlag (1983).

[8] VAN DER WAERDEN, B. L. *Moderne Algebra.* Erster Teil, zweite Auflage. Berlin, Verlag von Julius Springer (1937).

(Reçu le 3 septembre 1988)

François Sigrist

Institut de mathématiques et d'informatique
Université de Neuchâtel
Chantemerle 20
CH-2000 Neuchâtel (Suisse)