3. Un théorème de Galois

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 $ma'_i = ia_i$, 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*: