DES QUATRE OPÉRATIONS À LA NOTION DE GROUPE

Mémoire fondateur de CAUCHY

Etienne KOEHLER

Si la théorie des groupes est une découverte des temps modernes, elle est néanmoins l'héritière directe d'une longue ligne d'évolution. Son émergence est étroitement imbriquée entre la théorie des nombres et la résolution algébrique des équations, qui en est une des premières applications. En retour, la généralisation de la théorie de GALOIS *sera une importante voie de recherche en théorie des groupes.*

Les problèmes de calcul font partie, à côté des problèmes géométriques, des thèmes fondateurs des mathématiques. Au fil des temps, la notion de nombre s'est considérablement agrandie : les grecs ne concevaient pas les rapports comme des nombres. Néanmoins, l'insuffisance des nombres entiers à décrire le monde avait été prouvée, marquant l'échec du Pythagoricisme — la rumeur publique déclare même que la révélation de l'irrationnalité de $\sqrt{2}$ était frappée de la peine de mort (ce qui laisse songeur quand on pense au flot actuel des publications en théorie des nombres).

Pour des raisons essentiellement commerciales, à partir du Moyen Age, fut développée l'écriture décimale et la pratique des quatre opérations ; celles-ci maîtrisées, les frontières furent élargies du côté des nombres et on vit apparaître les nombres négatifs et fractionnaires pour calculer des parts d'héritage, des bilans entre pertes et profits, des rentes ... Les nombres "*imaginaires* " apparurent à la même époque pour des extractions de racine et les quatre opérations s'étendirent naturellement à ces nouveaux nombres sans qu'on en comprenne toujours très bien les fondements. L'exploration des nouveaux territoires prit deux cents ans.

GAUSS fut le premier à en sortir, tout d'abord en faisant des calculs sur les congruences (déjà esquissés par EULER) puis, étape fondamentale, en définissant une opération qui ne portait plus sur des nombres, mais sur des classes de formes quadratiques.

CAUCHY, lecteur assidu des '*Disquisitiones arithmeticae*' dont GAUSS est l'auteur, fut le second à définir une opération non-numérique et posa à cette occasion les fondations de la théorie des groupes finis. Cette opération, la composition des substitutions, fut étudiée dans un double mémoire présenté à l'Institut en 1812 et publié en 1815 dans le journal de l'Ecole Polytechnique : '*Mémoire sur le*

nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme'.

L'intérêt de ce mémoire est double. Outre qu'il étend la notion d'opération à des objets mathématiques qui ne sont pas des nombres, il apporte une contribution importante au problème de la résolution par radicaux des équations de degré supérieur à 4.

Pourtant, l'origine de ce mémoire se trouve dans les recherches de CAUCHY afin de démontrer un théorème de FERMAT, à savoir que "*tout nombre entier est la somme de n nombres n-gonaux*" (*). LAGRANGE avait prouvé que tout nombre était la somme de quatre carrés et GAUSS avait réglé le cas des nombres triangulaires grâce à sa théorie des formes trinaires. CAUCHY s'efforça de généraliser certains résultats de la théorie des formes, en particulier ceux concernant les déterminants. Il établit en général la formule $\det(AB) = (\det A)(\det B)$, ainsi que d'autres sur des déterminants extraits, trouvées indépendamment par BINET. Ces résultats sont présentés en relation avec le calcul des substitutions dans la deuxième partie du mémoire déjà cité. Mais c'est la première partie qui prend toute son importance dans une perspective historique, tant pour la généralisation de la notion d'opération que pour les travaux futurs de GALOIS.

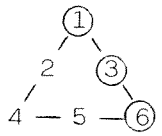
Dans cette première partie, CAUCHY démontre le théorème suivant : "*Le nombre des valeurs différentes d'une fonction non-symétrique de n quantités, ne peut s'abaisser au dessous du plus grand nombre premier p contenu dans n, sans devenir égal à 2* ". C'est une généralisation du cas particulier $n = 5$ démontré par RUFFINI qui avait pour cela explicité les cent vingt éléments de $\mathfrak{S}_5$ (**).

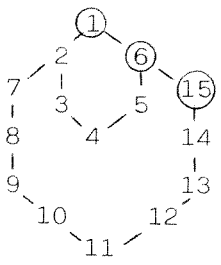
L'idée directrice de CAUCHY est d'étudier $\mathfrak{S}_n$ muni de la composition des substitutions et la méthode qui lui permet ensuite de conclure a été utilisée par GAUSS : former une partition d'un groupe selon un de ses sous-groupes. C'est ainsi qu'en

---

(*) Un nombre n-gonal est un nombre de la forme $p + (1/2)p(p-1)(n-2)$ avec p entier. Cette appellation résulte d'une disposition géométrique des naturels successifs sur le pourtour de n-gones emboîtés :

n=3 :1, 3, 6, 10 ...sont des nombres triangulaires
n=6 :1, 6, 15, 28 ...sont des nombres hexagonaux.





(**) $\mathfrak{S}_n$ est l'ensemble des permutations de n éléments. Cet ensemble contient $n!$ éléments.

préliminaire CAUCHY redémontre le théorème de LAGRANGE, à savoir qu'une fonction K de n variables étant donnée, le nombre de valeurs différentes de la fonction ne peut être qu'un diviseur du produit $1 \times 2 \times 3 \times \ldots \times n$ (*cf.* annexe 1). Puis CAUCHY définit ensuite ce qu'il appelle une substitution (*cf.* annexe 2). La démonstration du théorème s'organise alors en trois temps. Pour faciliter l'exposé, nous utiliserons les notations modernes suivantes : nous noterons σ une substitution, $< \sigma >$ l'ensemble des puissances successives de σ (donc le sous-groupe engendré par σ), Inv K l'ensemble des substitutions laissant K invariante et I la substitution identique.

a) Dans un premier temps, CAUCHY énonce le fait qu'il existe m tel que $< \sigma >= \{I, \sigma, \sigma^2, \ldots, \sigma^{m-1}\}$ avec $\sigma^m = I$, m étant appelé le degré de σ. Représentant alors les puissances successives de σ sur un cercle, il établit que si m et r sont premiers entre eux, $< \sigma^r >=< \sigma >$ et qu'en général $< \sigma^r > \subset < \sigma >$. Il compare ensuite deux partitions de $\mathfrak{S}_n$ d'une part au moyen des classes d'équivalence de la relation $\mathfrak{R}$:

$$\sigma_1 \, \mathfrak{R} \, \sigma_2 \Longleftrightarrow \sigma_1^{-1}\sigma_2 \in \text{Inv } K$$

(et soit M le nombre d'éléments d'une classe), d'autre part au moyen de celles de la relation $\mathfrak{R}'$:

$$\sigma_1 \, \mathfrak{R}' \, \sigma_2 \Longleftrightarrow \sigma_1^{-1}\sigma_2 \in < \sigma > .$$

Il suppose que σ est de degré p premier, donc qu'il y a $n!/p$ classes pour $\mathfrak{R}'$. Alors : $M > n!/p \Longrightarrow \exists r, \sigma^r \in \text{Inv } K$ donc $\sigma \in \text{Inv } K$, d'où sa conclusion. Si le nombre de valeurs différentes prises par K (c'est-à-dire $n!/M$) est strictement inférieur à p, alors K est invariante par toute substitution de degré p.

b) Dans un deuxième temps, il montre que toute substitution circulaire d'ordre p $(a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} a_4 \longrightarrow \ldots \xrightarrow{\sigma} a_p \xrightarrow{\sigma} a_1)$, notée $(a_1 a_2 \ldots a_p)$, est de degré p; que toute substitution d'ordre 3 est le produit de deux substitutions d'ordre p (dont nous noterons l'ensemble S_c^p) et que si K est invariante par toute substitution de S_c^p elle l'est aussi par toute substitution de S_c^3.

c) Dans un troisième temps, il remarque que $(\alpha\beta\gamma) = (\alpha\beta)(\beta\gamma)$ et que $(\alpha\beta)(\gamma\delta) = (\alpha\beta\gamma)(\beta\gamma\delta)$ c'est-à-dire, en langage moderne, que $\mathfrak{A}_n$ (ensemble des substitutions paires que CAUCHY déterminera dans la deuxième partie de son mémoire) est engendré par S_c^3, résultat déjà prouvé par RUFFINI pour $\mathfrak{S}_5$. Il en déduit que si $S_c^3 \subset \text{Inv } K$ alors $\mathfrak{A}_n \subset \text{Inv } K$ et, en faisant agir la transposition (1 2), que K prend alors deux valeurs différentes si K est non-symétrique et si le nombre de ses valeurs est inférieur à p.

Pour terminer cette première partie, CAUCHY établit le cas $n = 6$ d'un théorème que présentera en 1845 J. BERTRAND : "*Si $n \geq 5$, toute fonction de n quantités ayant plus de deux valeurs distinctes en admet au moins n*". La relation d'équivalence que CAUCHY envisage pour cela porte sur les indices $1, 2, \ldots n$ et non plus sur les substitutions, ce qui le conduit à une démonstration par exhaustion des cas nettement moins simple que celle qui précède.

Ce mémoire est essentiel pour les travaux de GALOIS dont les résultats sont trouvés, exprimés et montrés avec des groupes de substitution. En outre GALOIS, exprimant ses résultats dans ce qu'on appelle '*le premier mémoire*' cite explicitement CAUCHY : "*Or un groupe de permutations d'un nombre premier n de lettres ne peut se réduire à n permutations, à moins que l'une de ces permutations ne se déduise de l'autre par une substitution (circulaire) de l'ordre n (voir le mémoire de M.* CAUCHY — *Journal de l'école, 17)*". On voit ici que GALOIS est pressé par le temps : le terme circulaire a été rajouté et la *circularité* n'est nullement évidente.

CAUCHY cite simplement le fait qu'une substitution circulaire d'ordre n (n entier quelconque) est de degré n et (*cf.* annexe 3) que les orbites d'une substitution de degré n comportent n permutations.

Néanmoins, le résultat annoncé par GALOIS se déduit du texte de CAUCHY : dans la seconde partie CAUCHY montre que toute substitution est le produit de substitutions circulaires à supports disjoints, c'est-à-dire portant sur des ensembles disjoints d'indices, qui permutent donc entre elles. On voit alors (n étant premier) que chaque substitution circulaire est de degré n. Ces substitutions portant sur n lettres, elles ont toutes le même support (ces n lettres) et puisqu'elles ont aussi des supports disjoints, il n'y en a qu'une, c'est la une c'est-à-dire la substitution initialement donnée.

Les recherches en théorie des groupes ne commenceront à se développer qu'à partir de 1845. CAUCHY reprend vers cette époque ses travaux abandonnés depuis trente ans. LIOUVILLE publie en 1846 les manuscrits de GALOIS, jusque là restés inédits et à partir de 1861 commencent les travaux de JORDAN, pour la plupart réunis dans son '*traité des substitutions*'.

Quant à la théorie de GALOIS, il faut attendre les années 1910 pour que E. STEINITZ lui donne sa forme actuelle et mette en évidence les notions de séparabilité et de clôture algébrique. "*La théorie de* STEINITZ *permet aussi de représenter pour des corps quelconques la théorie de* GALOIS *comme l'avait déjà fait* DEDEKIND *pour les corps de nombres algébriques, le groupe de* GALOIS *devenant un groupe d'automorphismes d'un corps au lieu d'un groupe de permutations des racines*" (J. GUÉRINDON et J. DIEUDONNÉ, dans '*Abrégé d'histoire des mathématiques*').

ANNEXE 1

Théorème de LAGRANGE

Cela posé, K étant une fonction quelconque de l'ordre n, désignons par N le produit $1.2.3...n$, et par

$$A_1, A_2, A_3.....A_N,$$

les diverses permutations en nombre égal à N que l'on peut former avec les indices $1, 2, 3...n$, N sera le nombre total des valeurs de la fonction K relatives à ces diverses permutations.

Supposons que, parmi les valeurs possibles

$$K_1, K_2, K_3.....K_N$$

de la fonction donnée, plusieurs deviennent égales entre elles, en sorte qu'on ait, par exemple,

$$K_\alpha = K_\beta = K_\gamma = \&c....$$

Désignons par M le nombre total des valeurs K_α, K_β, K_γ, &c.... que l'on suppose ici égales entre elles. Les permutations relatives à ces valeurs, ou A_α, A_β, A_γ, &c..., seront aussi en nombre égal à M. Pour déduire toutes ces permutations d'une seule, par exemple, de A_α, il suffira d'échanger entre eux, d'une certaine manière, les indices qui, dans cette permutation, occupent certaines places; et l'on conçoit facilement que si ces changemens n'altèrent en rien la valeur correspondante K_α de la fonction K, cela tient non pas à la valeur même des indices, mais à la place que chacun d'eux occupe dans la permutation dont il s'agit.

Cela posé, soit K_λ une nouvelle valeur de K, qui ne soit pas égale à K_α; et désignons toujours par A_λ la permutation relative à K_λ. Si l'on fait subir simultanément aux indices qui occupent les mêmes places dans les permutations A_α et A_λ les changemens dont on vient de parler, la seconde permutation A_λ se trouvera successivement changée en plusieurs autres A_μ, A_ν, &c...., pendant que la première A_α deviendra successivement A_β, A_γ, &c.... ; et d'après le principe énoncé ci-dessus, il est évident que l'équation

$$K_\alpha = K_\beta = K_\gamma = \&c....;$$

entraînera celle-ci,

$$K_\lambda = K_\mu = K_\nu = \&c....$$

Il est aisé d'en conclure que, parmi les valeurs de K relatives à toutes les permutations possibles, savoir,

$$K_1, K_2, K_3 .....K_N,$$

le nombre de celles qui seront équivalentes à K_λ, sera le même que le nombre des valeurs équivalentes à K_α. Par suite, si l'on représente par R le nombre total des valeurs essentiellement différentes de la fonction K, M étant le nombre des valeurs équivalentes à K_α, RM sera le nombre total des valeurs relatives aux diverses permutations. On aura donc $RM = N$, et par suite

$$R = \frac{N}{M}.$$

Ainsi R, ou le nombre des valeurs différentes de la fonction K ne peut être qu'un diviseur de N, c'est-à-dire, du produit $1.2.3...n$.

ANNEXE 2

Voici les notations de CAUCHY concernant les substitutions et les permutations :

Soient A_1 et A_2 deux permutations de $1, 2, 3, \ldots n$; la substitution $\binom{A_1}{A_2}$ consiste à "*remplacer respectivement les indices compris dans la permutation* A_1, *par les indices correspondans compris dans la permutations* A_2" c'est-à-dire qu'en confondant A_i et la bijection associée, la substitution précédente vaut en notation actuelle $A_2 A_1^{-1}$ — puis il définit le produit (c'est-à-dire la composition) de deux substitutions, son sens d'écriture étant l'inverse de celui adopté actuellement; ainsi :

$$\binom{A_1}{A_2}\binom{A_2}{A_3} = [A_3 A_2^{-1}](A_2 A_1^{-1}) = \binom{A_1}{A_3}.$$

ANNEXE 3

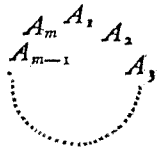
Supposons que l'on applique plusieurs fois de suite à la permutation A_1 la substitution $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}$, en sorte que cette substitution étant appliquée à la permutation A_1, donne pour résultat la permutation A_2; qu'étant appliquée à la permutation A_2, elle donne pour résultat la permutation A_3, &c..... La série des permutations

$$A_1,\ A_2,\ A_3,\ \&c.....$$

sera nécessairement composée d'un nombre fini de termes; et si l'on représente par m ce même nombre, et par A_m la dernière des permutations obtenues, la substitution $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}$ appliquée à cette dernière permutation reproduira de nouveau le terme A_1. Cela posé, si l'on range en cercle, ou plutôt en polygone régulier, les permutations

$$A_1,\ A_2,\ A_3 \ldots\ldots A_{m-1},\ A_m$$

de la manière suivante,



toutes les substitutions que l'on pourra former avec deux permutations prises à la suite l'une de l'autre et d'orient en occident dans le polygone dont il s'agit, seront équivalentes entre elles et à $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}$: et toutes celles que l'on pourra former avec deux permutations séparées l'une de l'autre par un nombre r de côtés dans ce même polygone, seront équivalentes à la puissance r de la substitution $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}$.

Il suit de ces considérations, 1.° que la puissance m de la substitution $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}$ est équivalente à la substitution identique $\begin{pmatrix} A_1 \\ A_1 \end{pmatrix}$; 2.° que x étant un nombre entier quelconque, $\begin{pmatrix} A_1 \\ A_t \end{pmatrix}^{mx}$ sera encore

une substitution identique; 3.° que, dans la même hypothèse, les substitutions $\begin{pmatrix} A_s \\ A_t \end{pmatrix}^{mx+r}$ et $\begin{pmatrix} A_s \\ A_t \end{pmatrix}^{r}$ sont équivalentes; 4.° que la notation $\begin{pmatrix} A_s \\ A_t \end{pmatrix}^{0}$ indique une substitution identique; 5.° que, parmi les substitutions dérivées de $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$, les seules qui soient différentes entre elles sont les puissances dont l'exposant est plus petit que m, ou, ce qui revient au même, les substitutions équivalentes à ces puissances, savoir;

$$\begin{pmatrix} A_1 \\ A_1 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \cdots\cdots \begin{pmatrix} A_1 \\ A_m \end{pmatrix}.$$

Le nombre de ces substitutions est comme celui des permutations $A_1, A_2, A_3 \ldots\ldots A_m$ égal à m. Ce nombre sera appelé le *degré* de la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$. Si l'on applique plusieurs fois de suite la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ à la permutation A_1, on commencera par obtenir la suite des permutations $A_1, A_2, A_3 \ldots\ldots A_m$; et lorsqu'on sera parvenu à ce point, les mêmes permutations se reproduiront dans le même ordre d'une manière périodique. C'est pourquoi je dirai que les permutations précédentes forment une période qui correspond à la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$. Cela posé, le degré d'une substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ indique à-la-fois la plus petite de ses puissances positives qui soit équivalente à une substitution identique, et le nombre des permutations comprises dans la période qui résulte de l'application de la substitution donnée à une permutation déterminée.