jacques DAUTREVAUX

SUBSTITUTIONS ET GROUPE SYMETRIQUE

BIBLIOTHEQUE DE TRAVAIL DU PROFESSEUR
DE MATHEMATIQUE

Publication de l'A.P.M.E.P.

MOTS I et II

L'Association des Professeurs de Mathématiques de l'Enseignement Public a entrepris de publier une série de brochures, intitulées MOTS, contenant des réflexions sur quelques mots-clés utilisés en mathématique à l'Ecole Elémentaire : égalité ; exemple et contre-exemple ; couple ; relation binaire ; nombre naturel ; entiers et rationnels ; nombre décimal, nombre à virgule ; fraction ; ensembles de nombres (brochure 1974) ; représentations graphiques ; application, fonction, bijection ; partition, équivalence ; partages ; divisibilité ; division euclidienne ; division (brochure 1975).

Chaque rubrique est détachable ; les feuilles, de format 15 X 21, sont perforées. La première brochure (1974) a 106 pages ; la suivante (1975) en a à peu près autant.

MOTS est une oeuvre collective ; l'équipe de rédaction, bénévole, constituée d'instituteurs, IDEN, professeurs (d'Ecole Normale, du Second Degré, du Supérieur) soumet ses projets à de nombreux instituteurs ; leurs avis lui sont précieux, surtout quand ils émanent de bacheliers littéraires qui n'ont pas eu l'occasion d'activité mathématique depuis leur sortie du lycée ou de l'école normale.

Sans être un manuel de mathématique, ni un lexique, MOTS permet au lecteur, à propos du vocabulaire rencontré dans les manuels scolaires ou les documents de formation permanente, de faire le point sur son évolution, sur les concepts et les idées qui s'y rattachent, et sur les notations utilisées.

Ces brochures, qui s'adressent aux enseignants, non aux élèves, sont vendues par l'APMEP aux prix suivants :

chacune des deux brochures : 6 F (port compris : 8 F)

Pour se les procurer, s'adresser à la Régionale (ou à la Départementale) de l'APMEP.

Sommaire

Introduction et bibliographie 4

I — PRELIMINAIRES
a) Généralités 5
b) Groupe opérant sur un ensemble, conjugaison 6

II — SUBSTITUTIONS, GROUPE SYMETRIQUE ET GROUPE ALTERNE 10

III — ETUDE DE LA STRUCTURE DU GROUPE SYMETRIQUE $\mathcal{S}_n$ 15
a) Conjugaison dans $\mathcal{S}_n$ 17
b) Centre de $\mathcal{S}_n$ 21
c) Sous-groupes distingués de $\mathcal{S}_n$ 21

IV — ETUDE DE LA STRUCTURE DU GROUPE ALTERNE $\mathcal{A}_n$ 25
a) Conjugaison dans $\mathcal{A}_n$ 28
b) Sous-groupes distingués de $\mathcal{A}_n$ 29
c) Centre de $\mathcal{A}_n$ 32

Conclusion 33

Appendice : Structure du groupe $0^+(\mathbf{R}^3)$ des rotations vectorielles de l'espace euclidien de dimension 3 35

INTRODUCTION

La théorie des groupes finis constitue en mathématiques un des problèmes encore les plus ouverts, justifiant l'intensité des recherches qui sont menées sur ce sujet par son utilisation dans des branches à priori très éloignées, par exemple en physique quantique. En outre, bien des aspects de cette théorie, en ce qui concerne tout au moins les groupes ayant un "petit" nombre d'éléments, sont facilement illustrables à tous les niveaux de l'enseignement. L'outil fondamental de la théorie est l'"Opération d'un groupe sur un ensemble" (cet ensemble peut être l'ensemble sous-jacent au groupe) et en particulier la conjugaison, dont l'emploi est presque systématique.

Les deux aspects essentiels sur lesquels travaillent les chercheurs depuis l'origine sont des aspects de représentations d'un groupe, soit comme *groupe de substitutions* — d'où l'intérêt d'étudier avant tout la structure du groupe symétrique et du groupe alterné — base de la théorie des équations algébriques, soit comme *groupe d'applications linéaires* d'un espace vectoriel dans lui-même (représentations linéaires).

C'est à ce premier aspect que, bien timidement, nous nous bornerons en étudiant la structure des groupes symétrique et alterné.

Bibliographie :

La théorie des groupes a fait l'objet dans ces dernières années de la publication de nombre d'ouvrages spécialisés d'un niveau élevé, les ouvrages plus élémentaires étant rares.

— Sur la théorie des groupes en général, les meilleurs ouvrages sont à l'heure actuelle :

1 MARSHALL HALL Jr : The theory of groups (Macmillan, 1959)

2 P. DUBREIL : Théorie des groupes (Dunod, 1972)

3 BURNSIDE : The theory of groups (Dover, 1955), plus difficile à lire, car cet ouvrage date de 1911.

— Sur les groupes de substitutions, plusieurs chapitres de 1 sont intéressants, mais aucun ouvrage d'ensemble n'existe depuis le monumental TRAITE DES SUBSTITUTIONS de Camille JORDAN et les ouvrages de J. de SEGUIER. A noter :

H. WIELANDT : Finite Permutation groups (Academic Press, 1964).

— On trouvera en outre des indications relativement élémentaires sur les extensions de corps dans :

4 LENTIN & RIVAUD : Leçons d'Algèbre moderne (Vuibert).

— Enfin, beaucoup de renseignements et d'illustrations de la théorie peuvent être trouvés dans l'excellent petit livre de notre collègue André WARUSFEL :

5 André WARUSFEL : Structures algébriques finies (Hachette, 1971)

I. PRELIMINAIRES

a) Généralités

Pour assurer la bonne compréhension de cet exposé, ont été rassemblées ici un certain nombre de définitions et propriétés utiles, à l'usage des collègues insuffisamment familiers avec les notions fondamentales de la théorie des groupes. On suppose évidemment connues les notions de groupe et de sous-groupe; ajoutons-y les notions particulières aux *groupes finis*, c'est-à-dire aux groupes dont le nombre des éléments est fini :

α) l'ordre d'un groupe fini est le nombre de ses éléments ; il en est de même d'ailleurs de l'ordre d'un sous-groupe, mais :

β) *Théorème de Lagrange* : l'ordre de tout sous-groupe d'un groupe G est un *diviseur* de l'ordre du groupe.

Sauf exception, la loi de composition d'un groupe est notée multiplicativement, et un groupe est *abélien* si cette loi est commutative. Rappelons qu'il est permis d'utiliser pour la loi de composition d'un groupe la notation additive seulement dans le cas où le groupe est abélien : c'est le cas de $\mathbf{Z}$ ou des groupes $\mathbf{Z}/n\mathbf{Z}$ (n entier), groupes pour lesquels la loi de composition est naturellement l'addition.

Si σ est un élément d'un groupe fini G, l'ensemble des puissances successives de σ est lui-même fini : il en résulte l'existence d'entiers relatifs $k \in \mathbf{Z}$ tels que $\sigma^k = 1$ (ainsi est noté l'élément neutre du groupe), et, si n est le plus petit de ceux des entiers k qui sont strictement positifs, ceux qui possèdent la

propriété énoncée sont tous les multiples de n. n est appelé l'*ordre* de l'élément σ, l'ensemble de toutes les puissances de σ est : $\Sigma = \{1, \sigma, \sigma^2, \sigma^3, ..., \sigma^{n-1}\}$, et il est clair que Σ est un sous-groupe de G : c'est le plus petit sous-groupe de G contenant σ, c'est-à-dire le sous-groupe engendré par σ. Par définition un tel sous-groupe est dit cyclique, d'après la définition :

Un groupe cyclique est un groupe qui peut être engendré par un seul élément (qu'on appelle un "générateur" du groupe).

Le CENTRE d'un groupe est l'ensemble, noté Z(G), des éléments de G qui commutent avec tous les éléments de G ; c'est un sous-groupe de G (car il contient toujours l'élément neutre de G), et même un sous-groupe distingué. Lorsque le groupe G est abélien, son centre Z(G) coïncide avec G.

Un sous-groupe H de G est dit *distingué* (ou encore *normal*) si, pour tout élément x de ce sous-groupe H, et pour tout élément σ de G, le produit $\sigma^{-1}x\sigma$ est encore un élément de H. C'est ainsi qu'on vérifie que le centre d'un groupe est distingué, et que, si le groupe G est abélien, tout sous-groupe est distingué.

Enfin un *groupe simple* est un groupe ne possédant aucun sous-groupe distingué non trivial (on remarque bien que les deux sous-groupes triviaux $\{1\}$ et G lui-même, du groupe G, sont tous deux distingués).

N.B. Dans tout ce qui suit, le mot "entier" est toujours pris dans le sens de "entier naturel non nul" ou de "naturel non nul".

b) **Groupe opérant sur un ensemble, conjugaison**

On dit qu'un groupe G "*opère*" sur un ensemble E lorsqu'il existe une application de $G \times E$ dans E (c'est l'*opération de G sur E*) dans laquelle un élément σ de G agit sur l'élément x de E en le transformant en un élément de E noté $\sigma \cdot x$: $(\sigma, x) \longmapsto \sigma \cdot x$, sous réserve des deux propriétés suivantes :

— l'élément neutre du groupe G (noté ici 1) agit sur E comme l'identité, c'est-à-dire que :

$$1 \cdot x = x \text{ , pour tout élément } x \text{ de E ;}$$

— l'opération doit être compatible avec la loi de groupe G : pour σ et τ dans G, on doit toujours avoir :

$$\sigma \cdot (\tau \cdot x) = (\sigma\tau) \cdot x \text{ , pour tout élément } x \text{ de E.}$$

Cette relation exprime que la loi de groupe de G est identifiable à la composition des applications de E dans E. Il en résulte que, si x et y sont deux éléments de E tels qu'il existe un élément σ de G tel que : $y = \sigma \cdot x$, alors on aura : $x = \sigma^{-1} \cdot y$, où σ^{-1} désigne l'inverse dans le groupe G de l'élément σ.

On peut alors définir sur l'ensemble une relation binaire $\mathcal{R}$ par :

$$y \mathcal{R} x \quad \text{si et seulement si il existe } \sigma \in G \text{ tel que } y = \sigma \cdot x \text{ ;}$$

cette relation est, d'après ce qui précède, une relation d'équivalence puisque réflexive ($1 \cdot x = x$, donc $x \mathcal{R} x$ pour tout élément x de E), symétrique ($y = \sigma \cdot x$ entraînant $x = \sigma^{-1} \cdot y$, donc $y \mathcal{R} x$ entraîne $x \mathcal{R} y$) et transitive ($z \mathcal{R} y$ et $y \mathcal{R} x$ entraînant $z \mathcal{R} x$ puisque, si $z = \tau \cdot y$ et $y = \sigma \cdot x$, on a : $z = \tau \cdot (\sigma \cdot x) = (\tau\sigma) \cdot x$). Cette relation d'équivalence partage E en classes d'équivalence qu'on appelle des ORBITES, et il est clair que l'orbite $\gamma(x)$ contenant le point x est l'ensemble :

$$\gamma(x) = \{\sigma \cdot x \quad \text{pour tous les éléments } \sigma \text{ de G}\}.$$

Lorsque le groupe G est fini et possède g éléments, alors chaque orbite contient au plus g éléments ; en fait, si x est un élément donné de E et si y est un élément de l'orbite $\gamma(x)$, il peut être obtenu à partir de x de plusieurs façons différentes : si σ et τ sont deux éléments de G tels que $y = \sigma \cdot x = \tau \cdot x$, on a : $(\sigma^{-1}\tau) \cdot x = x$, de sorte que $\sigma^{-1}\tau$ est un élément de l'ensemble S(x) des éléments de G qui fixent x :

$$S(x) = \{\sigma \in G \quad \text{tels que} \quad \sigma \cdot x = x\}$$

On vérifie aisément que S(x) est un sous-groupe de G ; soit s le nombre des éléments de S(x), il est clair que l'élément y de $\gamma(x)$ est obtenu à partir de x de s façons différentes, de sorte que le nombre, p, des éléments distincts de $\gamma(x)$, vérifie la relation : $g = sp$, et que par suite p est un diviseur de g (on sait que s est aussi un diviseur de g, puisque S(x) est un sous-groupe, mais en fait cette propriété est ici superflue).

Quand le groupe G est fini, le nombre des éléments de chaque orbite est un diviseur de l'ordre du groupe G.

Lorsqu'une orbite n'a qu'un seul élément : $\gamma(x) = \{x\}$, cet élément est *fixé* par G (c'est un "point fixe" de l'opération de G

sur E), car alors on a : $\sigma \cdot x = x$ pour tout élément σ de G (on peut dire aussi que $S(x) = G$).

Il est évident que, si l'ensemble E est fini lui aussi, la somme des nombres d'éléments de toutes les orbites est égale au nombre des éléments de E, puisque les orbites en constituent une partition.

Un des exemples les plus importants de cette notion d'opération d'un groupe sur un ensemble est la *conjugaison*, qui joue un rôle important dans la théorie des groupes. Si x et σ sont deux éléments d'un groupe G, le *conjugué* de x par σ est l'élément, noté x^σ, et égal au produit $\sigma^{-1}x\sigma$, et qui n'est distinct de x que si $x\sigma \neq \sigma x$, ce qui ne peut se produire que dans un groupe non abélien (c'est-à-dire non commutatif). On peut aussi noter que $x^\sigma = x$ caractérise le fait que σ et x commutent.

Un groupe G opère sur lui-même par conjugaison (E est alors l'ensemble sous-jacent à G) par : $\sigma \cdot x = x^{\sigma^{-1}}$ ($\sigma \in G$, $x \in G$ considéré comme l'ensemble E précédent), et on vérifie bien que les conditions énoncées plus haut pour avoir une opération sont bien remplies :

$$1 \cdot x = x^1 = x \quad \text{pour tout } x,$$

car l'élément neutre 1 du groupe commute avec tout élément de G

$$\text{et} \quad \sigma \cdot (\tau \cdot x) = (\tau \cdot x)^{\sigma^{-1}} = (x^{\tau^{-1}})^{\sigma^{-1}} = \sigma(\tau x \tau^{-1})\sigma^{-1} = (\sigma\tau)x(\tau^{-1}\sigma^{-1})$$
$$= (\sigma\tau)x(\sigma\tau)^{-1} = x^{(\sigma\tau)^{-1}} = (\sigma\tau)\cdot x \quad ,$$

et ceci est vrai quels que soient les éléments x, σ et τ de G.

Les orbites obtenues s'appellent les *classes de conjugaison* du groupe G, l'orbite d'un élément x est alors l'ensemble des conjugués de x par tous les éléments de G :

$$\gamma(x) = \{ x^\sigma \quad \text{pour tous les éléments } \sigma \text{ de G} \} .$$

— Lorsque le groupe est fini, le nombre des éléments contenus dans chaque classe de conjugaison est un diviseur de l'ordre du groupe ;

— et de plus, la somme des nombres d'éléments des diverses classes de conjugaison de G est égale à l'ordre de G, puisque les classes de conjugaison réalisent une partition de G ;

— si une classe de conjugaison $\gamma(x) = \{x\}$ ne contient qu'un seul élément x de G, cet élément x commute avec tous les éléments de G ; x est alors un élément du *centre de* G ;

— l'élément neutre 1 du groupe G appartient toujours à son centre, de sorte que la classe de conjugaison de l'élément 1 ne contient jamais d'autre élément que 1 : $\gamma(1) = \{1\}$ dans n'importe quel groupe ;

— si un sous-groupe distingué H de G contient un élément x, il contient aussi, par suite de la définition d'un sous-groupe distingué, tous les conjugués de x, donc aussi l'ensemble de ses conjugués, soit la classe de conjugaison de x, ce qui peut s'énoncer :

> Si un sous-groupe distingué de G contient un élément x, il contient aussi en entier la classe de conjugaison de x.

Remarque 1 :

[Un groupe dont le nombre des éléments est un entier premier p est nécessairement abélien.

En effet, le nombre des éléments de chaque classe de conjugaison de G est un entier divisant p, celui-ci ne pouvant donc être que 1 ou p. La somme de tous ces entiers étant p, on ne peut avoir à priori que deux possibilités :

— ou bien une seule classe de conjugaison contenant p éléments ;

— ou bien p classes de conjugaison ne contenant chacune qu'un seul élément de G.

Or, la première de ces hypothèses est absurde car on a dit plus haut qu'il existait obligatoirement une classe de conjugaison au moins ne contenant qu'un seul élément, celle qui correspond à l'élément neutre 1. Il en résulte que chacun des éléments de G commute avec tous les autres, et par suite que le groupe est abélien.

Remarque 2 :

On peut généraliser la démonstration précédente en considérant un groupe G dont l'ordre est une puissance d'un entier premier p, donc un entier de la forme p^α, où p est premier.

Le nombre des éléments de chaque classe de conjugaison est en effet un entier diviseur de p^α, et il ne peut être que 1 ou un multiple de p : si n est le nombre de classes de conjugaison dont le nombre des éléments est égal à 1, on peut écrire que la somme des nombres d'éléments de toutes les classes de conjugaison est égale à $p^\alpha = n +$ une somme de multiples de p, et cette relation

exige que n soit égal, soit à 0, soit à un multiple de p ; comme précédemment, $n \geqslant 1$, de sorte que n est nécessairement un multiple de p, d'où $n \geqslant p$.

De l'interprétation des éléments de G dont la classe de conjugaison ne contient qu'un seul élément on tire l'intéressante propriété :

[Si G est un groupe d'ordre p^α (p premier), son centre contient au moins p éléments.

En fait d'ailleurs l'ordre du centre est un diviseur de p^α, soit un entier de la forme p^β avec $1 \leqslant \beta \leqslant \alpha$.

II. SUBSTITUTIONS, GROUPE SYMETRIQUE et GROUPE ALTERNE

Si E est un ensemble fini ayant n éléments, on sait qu'on appelle "substitution sur E" toute bijection de E sur E, et que l'ensemble de toutes ces substitutions constitue un groupe fini, possédant $n!$ éléments, noté $\mathcal{S}_n$ et appelé le *GROUPE SYMETRIQUE de degré* n.

Toute suite ordonnée des n éléments de E est une "permutation" : il en existe $n!$, et toute substitution transforme une permutation en une autre permutation. D'ordinaire on numérote les éléments de E, de 1 à n, et on identifie une permutation à une suite des n entiers $1, 2, 3, \ldots, n$, pris dans un certain ordre, et dans cette suite on a une inversion toutes les fois qu'après (c'est-à-dire à droite) un entier on en trouve un plus petit. La *signature* d'une substitution σ de $\mathcal{S}_n$ est l'entier $(-1)^N$, où N est le nombre d'inversions que l'action de σ introduit dans la suite $(1, 2, 3, \ldots, n)$ des n premiers entiers rangés dans l'ordre naturel. La considération de la signature permet de distinguer les *substitutions paires*, dont la signature est $+1$, et les *substitutions impaires*, dont la signature est -1. Le produit de deux substitutions σ et τ, noté multiplicativement $\sigma\tau$, doit être compris à la manière d'une composition d'applications, c'est-à-dire que $\sigma\tau$ appliqué à une permutation quelconque donne le même résultat qu'en appliquant d'abord τ, puis, au résultat obtenu, σ. On montre assez aisément que la signature d'un produit de substitutions est égale au produit des signatures, de sorte que le produit de

deux substitutions paires ou impaires est une substitution paire, et que le produit de deux substitutions dont l'une est paire et l'autre impaire est une substitution impaire ; comme l'identité de E est manifestement une substitution paire, la substitution réciproque (ou "inverse" en vertu de la notation multiplicative) d'une substitution σ a même parité que σ. Il en résulte que l'ensemble des substitutions paires est un sous-groupe de $\mathcal{S}_n$ appelé le *GROUPE ALTERNE de degré* n ; ce sous-groupe contient exactement $\frac{1}{2}n!$ éléments, et il est distingué dans $\mathcal{S}_n$; on le note $\mathcal{A}_n$.

La manière la plus simple d'étudier les substitutions sur un ensemble fini E est d'identifier E à l'ensemble $\{1, 2, 3, \ldots, n\}$ des n premiers entiers (qui est l'ensemble d'indexation de E) et de déterminer un élément σ de $\mathcal{S}_n$ au moyen de l'image $(a_1, a_2, a_3, \ldots, a_n)$ qu'il donne de la permutation $(1, 2, 3, \ldots, n)$, avec naturellement $a_i = \sigma(i)$.

Parmi les substitutions de $\mathcal{S}_n$, nous ferons une place spéciale aux *CYCLES* ; un CYCLE est un élément γ de $\mathcal{S}_n$ satisfaisant aux conditions suivantes : il existe une partie $\{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$ de $E = \{1, 2, 3, \ldots, n\}$ pouvant être ordonnée (indexation faite par les entiers $1, 2, \ldots, \ell$) de telle sorte que :

$$\begin{cases} \gamma(x) = x & \text{si } x \notin \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}, \\ \gamma(\alpha_i) = \alpha_{i+1} & \text{si } i \in \{1, 2, \ldots, \ell - 1\} \\ \gamma(\alpha_\ell) = \alpha_1 & \end{cases}$$

ℓ est la *longueur du cycle* γ ; évidemment $1 \leqslant \ell \leqslant n$.

Un cycle de longueur 1 est toujours l'identité de E ; de fait, la définition donnée suppose à proprement parler $\ell \geqslant 2$, mais la cohérence des raisonnements exige la considération de cycles de longueur 1.

Un cycle de longueur 2 est une *transposition* ; la transposition notée (i,j) est celle qui dans l'ensemble E échange les lettres i et j et conserve toutes les autres.

Un cycle de longueur n n'est autre que ce qui est appelé vulgairement une "permutation circulaire", dénomination impropre que nous nous garderons bien d'utiliser.

La notation habituelle pour représenter le cycle γ dont il a été question ci-dessus est : $\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$, dont la signification est évidente ; les autres éléments de E sont fixés par γ.

Si par exemple $E = \{1, 2, 3, 4, 5, 6\}$, le cycle $\gamma = (1, 3, 4, 6)$ est la substitution définie par :

$$\gamma(1) = 3 \qquad \gamma(2) = 2 \qquad \gamma(3) = 4$$
$$\gamma(4) = 6 \qquad \gamma(5) = 5 \qquad \gamma(6) = 1$$

et la longueur d'un tel cycle est $\ell = 4$.

Revenons-en au cycle γ opérant sur l'ensemble E ordonné de telle sorte que sur l'ensemble des indices $\{1,2,3,\ldots,\ell-1,\ell,\ell+1,\ldots,n\}$ ce cycle soit représenté par : $\gamma = (1,2,3,\ldots,\ell)$; alors l'image de la permutation naturelle (entiers $1, 2, \ldots, n$ rangés dans l'ordre naturel) est la permutation $(2,3,4,\ldots,\ell,1,\ell+1,\ldots,n)$, qui présente exactement $\ell - 1$ inversions et par suite :

— un cycle de longueur paire est une substitution impaire ;
— un cycle de longueur impaire est une substitution paire.

Ainsi, toute transposition est une substitution impaire, l'identité ou un cycle de longueur 3 est une substitution paire.

Lemme 1 :

> Toute substitution est décomposable en un produit de transpositions.

Ce théorème se démontre classiquement par une récurrence descendante sur le nombre d'éléments de l'ensemble E fixés par la substitution σ qu'on a choisie dans le groupe $\mathcal{S}_n$.

— Lorsque la substitution fixe les n éléments de E (ou, ce qui est équivalent, lorsqu'elle en fixe $n-1$), c'est l'identité. Or l'identité peut s'écrire comme produit d'une transposition quelconque et d'elle-même, et c'est bien un produit de transpositions.
— Lorsque la substitution fixe $n-2$ éléments de E, elle agit sur deux d'entre eux seulement, et par suite elle est une transposition.

Le théorème est donc vrai pour toute substitution fixant au moins $n-2$ éléments de E. On suppose alors (hypothèse de récurrence) le théorème vrai pour toute substitution fixant $n-p$ ($2 \leqslant p < n$, p fixé) éléments de E, et on suppose que la substitution σ fixe $n-p-1$ éléments de E. On peut alors toujours numéroter les éléments de E de telle sorte que les indices des éléments de E modifiés par σ soient $1, 2, \ldots, p, p+1$, les éléments

de E ayant pour indices $p+2, p+3, \ldots, n$ (s'il en existe) étant fixés par σ. Soit τ la transposition échangeant $p+1$ et $\sigma(p+1)$: alors $\tau\sigma$ est une substitution fixant $p+1$ (et aussi les éléments déjà fixés par σ), de sorte que $\tau\sigma$ est une substitution fixant $n-p$ éléments de E, à laquelle l'hypothèse de récurrence s'applique : $\tau\sigma$ se décompose en un produit $\tau\sigma = \tau_1 \tau_2 \ldots \tau_k$ de transpositions τ_i, de sorte que, puisque $\tau^{-1} = \tau$, on a : $\sigma = \tau\tau_1 \tau_2 \ldots \tau_k$, qui est donc aussi un produit de transpositions.

Remarque 1 :

La décomposition n'est pas unique en général, mais la parité du nombre de transpositions composantes est la même que la parité de σ. De plus, les transpositions obtenues ne commutent pas en général et l'ordre doit être respecté.

Remarque 2 :

Du fait du lemme 1, on dit que :

> Le groupe symétrique est engendré par les transpositions.

Par suite, tout sous-groupe de $\mathcal{S}_n$ contenant *toutes* les transpositions coïncide avec $\mathcal{S}_n$.

Lemme 2 :

> Toute substitution paire est décomposable en un produit de cycles de longueur 3.

La démonstration utilise une récurrence analogue à la précédente. On suppose évidemment $n \geqslant 3$.

— Lorsque la substitution paire fixe les n éléments de E (ou, ce qui est équivalent, lorsqu'elle en fixe $n-1$), il s'agit de l'identité, produit d'un cycle de longueur 3 et de son inverse, qui est aussi un cycle de longueur 3 : on a bien un produit de cycles de longueur 3.
— Lorsque la substitution fixe $n-2$ éléments de E, elle fixe également les deux autres, sinon elle serait une transposition, qui est une substitution impaire : on a encore une fois l'identité.
— Lorsque la substitution paire fixe $n-3$ éléments de E, elle n'en fixe aucun des trois autres, et elle est par conséquent nécessairement un cycle de longueur 3.

Le théorème étant vrai pour toute substitution fixant au moins $n-3$ éléments de E, on suppose alors (hypothèse de récurrence)

qu'il l'est pour toute substitution fixant au moins $n-p$ éléments de E. Soit alors σ une substitution paire fixant $n-p-1$ éléments de E ($3 \leqslant p < n$, p fixé) : on numérote les éléments de E de telle sorte que les indices des éléments modifiés par σ soient $1, 2, \ldots, p, p+1$, de sorte que les éléments d'indices $p+2, p+3, \ldots, n$, s'il en existe, sont fixés par σ. Soit γ le cycle $(1, \sigma(p+1), p+1)$: la substitution $\gamma\sigma$ est une substitution paire (produit de deux substitutions paires), et elle fixe $p+1$, ainsi d'ailleurs aussi que les éléments fixés par σ : c'est donc une substitution paire fixant au moins $n-p$ éléments de E, et elle se décompose en un produit $\gamma\sigma = \gamma_1 \gamma_2 \ldots \gamma_k$ de cycles de longueur 3. Comme γ^{-1} est aussi un cycle de longueur 3, on voit que : $\sigma = \gamma^{-1} \gamma_1 \gamma_2 \ldots \gamma_k$ est bien aussi un produit de cycles de longueur 3.

Remarque 3 :

La décomposition n'est pas unique en général. De plus, les cycles obtenus ne commutent pas en général et l'ordre doit être respecté.

Remarque 4 :

Du fait du lemme 2, on dit que :

Le groupe alterné est engendré par les cycles de longueur 3.

Par suite, tout sous-groupe de $\mathcal{A}_n$ contenant *tous* les cycles de longueur 3 coïncide avec $\mathcal{A}_n$.

Ordre d'un cycle.

L'ordre d'un élément σ d'un groupe G dont l'élément neutre est noté e est le plus petit des entiers strictement positifs p tels que $\sigma^p = e$.

Cet ordre existe toujours lorsque le groupe G est fini, et il est un diviseur de l'ordre (ou nombre d'éléments) du groupe G ; la terminologie est justifiée par le fait que l'ordre de l'élément σ est aussi l'ordre du sous-groupe cyclique engendré par σ (cf. la note annexe à la fin de cet exposé). Si γ est un cycle de longueur ℓ, il est clair que γ^ℓ est l'identité, et que pour tout entier $p < \ell$, γ^p n'est pas l'identité. Par suite :

Un cycle de longueur ℓ est un élément d'ordre ℓ dans $\mathcal{S}_n$.

III. ETUDE DE LA STRUCTURE DU GROUPE SYMETRIQUE $\mathcal{S}_n$

On considérera maintenant le groupe $\mathcal{S}_n$ des substitutions d'un ensemble fini $E = \{1, 2, 3, \ldots, n\}$ dont les n éléments seront appelés des "lettres" représentées d'ailleurs par les entiers qui les indexent.

Il peut arriver qu'une substitution σ laisse fixes certaines lettres de l'ensemble E : on appelle alors *support* de la substitution σ le complémentaire dans E de l'ensemble des lettres fixées par σ (si l'on veut, le support de σ est exactement l'ensemble des lettres qui sont déplacées par la substitution σ) ; la restriction de σ à son support S est une substitution de l'ensemble S, et le groupe des substitutions de S (qui, si S contient p lettres, est le groupe symétrique $\mathcal{S}_p$) peut être identifié à un sous-groupe de $\mathcal{S}_n$, groupe des substitutions de E ; de sorte que par abus de langage on identifie souvent une substitution de E avec sa restriction à son support.

On vérifie de façon immédiate que, si σ et τ sont deux substitutions de E (c'est-à-dire deux éléments de $\mathcal{S}_n$) dont les supports sont deux sous-ensembles *disjoints* de E, alors σ et τ commutent : $\sigma\tau = \tau\sigma$.

On dit alors que σ et τ sont à supports disjoints, ou, par abus de langage, que σ et τ sont deux *substitutions disjointes*, de sorte que :

Deux éléments disjoints de $\mathcal{S}_n$ commutent.

Soit alors σ un élément quelconque de $\mathcal{S}_n$, Σ le sous-groupe cyclique engendré par σ ; l'ordre du sous-groupe Σ est en même temps l'ordre de l'élément σ. Ce sous-groupe opère naturellement sur l'ensemble E des indices par :

$$\text{pour } s \in \Sigma \quad \text{et pour } i \in E \ : \quad s.i = s(i)$$

On a bien une opération car les deux conditions pour qu'il en soit ainsi se trouvent vérifiées, puisque la substitution identique e, qui est un élément de tout sous-groupe de $\mathcal{S}_n$, opère bien comme l'identité de E, et que, si s et t sont deux éléments de Σ, on a :

$$t \,.\, (s.i) = t[s(i)] = (t \circ s)\,(i) = (ts) \,.\, i$$

en revenant à la notation multiplicative adoptée pour le groupe symétrique.

Dès lors, cette opération partage l'ensemble en orbites, le nombre des éléments de chaque orbite est un diviseur de l'ordre de Σ, et la somme des nombres d'éléments de toutes les orbites est égale à n, les orbites ne contenant qu'un seul élément correspondant naturellement aux éléments de E fixés par σ, donc aussi par tout $s \in \Sigma$.

Il est remarquable de constater que la restriction de σ à l'une quelconque des orbites est un *cycle* dont la longueur est égale au nombre des éléments de cette orbite. En effet, d'après la définition de l'orbite et compte tenu de ce que les éléments de Σ sont σ, $\sigma^2, \ldots, \sigma^{p-1}$, e (avec $\sigma^p = e$, p étant l'ordre de Σ ou de σ), l'orbite d'un élément a de E est l'ensemble de ceux des éléments a, $\sigma(a)$, $\sigma^2(a)$, ..., $\sigma^{p-1}(a)$ qui sont distincts deux à deux ; en fait on vérifie facilement que, si ℓ est *le plus petit* des entiers strictement plus grands que 1 tels que $\sigma^\ell(a)$ soit un élément appartenant à l'ensemble $\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{\ell-1}(a)\}$, on a nécessairement $\sigma^\ell(a) = a$, et le nombre d'éléments de l'orbite de a est exactement égal à ℓ, qui est dès lors un diviseur de l'ordre p de σ. Alors la restriction de σ à cette orbite est un cycle de longueur ℓ qui peut être considéré comme un élément de $\mathcal{S}_n$ ayant pour support cette orbite. Si nous avons k orbites, à chacune d'elles on pourra associer un cycle de $\mathcal{S}_n$, ayant cette orbite comme support, et dont la restriction à son support coïncide avec la restriction de σ, et il est alors clair que σ se présente comme le produit (dans le groupe $\mathcal{S}_n$) de tous ces cycles ; de plus, puisque tous les cycles obtenus sont deux à deux disjoints, ils commutent deux à deux, et la décomposition est évidemment unique.

Théorème :

> Toute substitution $\sigma \in \mathcal{S}_n$ est *de façon unique* (à l'ordre des facteurs près) un produit de cycles disjoints.

Soit : $\sigma = c_1\, c_2 \ldots c_k$.

Si ℓ_i est la longueur du cycle c_i, alors on peut toujours, puisque les cycles commutent deux à deux, indexer ces cycles de telle sorte que :

$$\ell_1 \geqslant \ell_2 \geqslant \ldots \geqslant \ell_k \geqslant 1$$

(classement par longueurs décroissantes),

avec : $\ell_1 + \ell_2 + \ldots + \ell_k = n$.

De plus, chacun des ℓ_i étant un diviseur de l'ordre de σ, il apparaît aisément que l'ordre de la substitution σ est égal au plus petit commun multiple (PPCM) des ordres des cycles composants, c'est-à-dire des ℓ_i.

Définition :

> Le k-uplet $[\ell] = (\ell_1, \ell_2, \ldots \ell_k)$ est appelé la *formule* de la substitution σ.

On suppose évidemment $\ell_1 \geqslant \ell_2 \geqslant \ldots \geqslant \ell_k \geqslant 1$, et σ est alors complètement déterminé par la donnée supplémentaire des supports des cycles composants (ces supports doivent former une partition de E, et respecter les nombres d'éléments correspondant à la formule de σ, abstraction faite évidemment des éléments de E fixés par σ).

Conformément à ce qui a été dit dans le préambule, il faut, afin d'assurer la cohérence des raisonnements, associer à chaque orbite ne contenant qu'un seul élément un *cycle de longueur 1*, restriction à cet élément de l'identité e de $\mathcal{S}_n$.

Exemples :

La formule de l'identité e est (1,1,1,....,1) (avec n fois le nombre 1), que pour simplifier on écrit souvent sous la forme 1^n.

La formule d'une transposition est (2,1,1,....,1) avec $(n-2)$ fois le nombre 1, soit sous la forme symbolique 2.1^{n-2}.

La formule d'un cycle de longueur ℓ est $(\ell,1,1,\ldots,1)$ avec $(n-\ell)$ fois le nombre 1, dont l'écriture symbolique est $\ell.1^{n-\ell}$ $(2 \leqslant \ell \leqslant n)$, la formule d'un cycle de longueur n est (n), soit symboliquement n.

En notation symbolique, avec $n = 15$, la formule $4.3^2.2.1^3$ représente une substitution de formule (4,3,3,2,1,1,1) qui fixe donc trois points de E.

a) **Conjugaison dans $\mathcal{S}_n$**

1*) *Conjugué d'un cycle :*

Soit $\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ un cycle de longueur ℓ, écrit avec

les notations du début, sans écrire explicitement les éléments de E fixés par γ, et σ un élément quelconque du groupe symétrique $\mathcal{S}_n$. Alors on vérifie aisément que (selon les notations antérieures) $\sigma\cdot\gamma = \gamma^{\sigma^{-1}} = \sigma\gamma\sigma^{-1}$ n'est autre que le cycle $(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_\ell))$ de même longueur que γ, car :

si x n'est pas un des ℓ éléments $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_\ell)$, alors $\sigma^{-1}(x)$ n'est pas l'un des éléments $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ et est donc fixé par γ, de sorte que : $\sigma\,\gamma\,\sigma^{-1}(x) = \sigma\,\gamma\,[\sigma^{-1}(x)] = \sigma[\sigma^{-1}(x)] = x$, de sorte que x est fixé par $\sigma\cdot\gamma$; par contre :

si $x = \sigma(\alpha_i)$ pour quelque i $(1 \leqslant i \leqslant \ell)$, alors $\sigma^{-1}(x) = \alpha_i$ et $\gamma(\alpha_i) = \alpha_{i+1}$ (en convenant de prendre $\ell + 1 = 1$), et on a dans ce cas $(\sigma\cdot\gamma)(x) = \sigma\,\gamma\,\sigma^{-1}[\sigma(\alpha_i)] = \sigma\,\gamma(\alpha_i) = \sigma(\alpha_{i+1})$, avec la convention précédente naturellement.

Réciproquement, deux cycles de même longueur sont conjugués : en effet si on envisage les deux cycles :

$$\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$$
$$\text{et} \quad \gamma' = (\beta_1, \beta_2, \ldots, \beta_\ell),$$

on aura bien : $\gamma' = \sigma\cdot\gamma = \gamma^{\sigma^{-1}}$ pourvu que la substitution σ soit choisie de telle sorte que :
$\sigma(\alpha_1) = \beta_1$, $\sigma(\alpha_2) = \beta_2$, ..., $\sigma(\alpha_\ell) = \beta_\ell$.

De plus, si $\ell \leqslant n-2$, on pourra toujours supposer que la substitution σ trouvée est *paire*, au besoin en la composant avec une transposition τ disjointe de γ (c'est-à-dire agissant sur deux des éléments de E fixés par γ) car $(\sigma\tau)\cdot\gamma = \sigma\cdot(\tau\cdot\gamma) = \sigma\cdot\gamma$ puisque τ commute avec γ, leurs supports étant disjoints : alors, si σ est impaire, $\sigma\,\tau$ est paire. Il en est de même lorsque $\ell = n-1$ où n est un entier pair, car alors le cycle γ est une substitution impaire, et, comme γ commute évidemment avec lui-même, on aura : $(\sigma\gamma)\cdot\gamma = \sigma\cdot(\gamma\cdot\gamma) = \sigma\cdot\gamma$ et, si σ est impaire, $\sigma\gamma$ est paire.

Par suite : deux cycles de même longueur ℓ sont conjugués, et, sauf le cas où ℓ est celui des deux entiers n ou $n-1$ qui est impair, la conjugaison peut être obtenue au moyen d'une substitution *paire*.

2*) *Conjuguée d'une substitution quelconque :*

Une substitution quelconque s peut s'écrire de façon unique comme un produit de cycles disjoints : $s = c_1 c_2 \ldots c_k$, où c_i a

pour longueur $\ell_i \geqslant 2$, en n'écrivant pas les cycles de longueur 1 qui sont identifiables à l'identité e, élément neutre de $\mathcal{S}_n$. Si σ est une substitution fixée, on aura :

$$\begin{aligned}\sigma\cdot s = s^{\sigma^{-1}} &= \sigma s \sigma^{-1} = \sigma(c_1 c_2 \ldots c_k)\sigma^{-1} \\ &= (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_k \sigma^{-1}) \\ &= (\sigma\cdot c_1)(\sigma\cdot c_2) \ldots (\sigma\cdot c_k),\end{aligned}$$

où $\sigma\cdot c_i$ est aussi un cycle de longueur ℓ_i ; le nombre des éléments de E fixés par $\sigma\cdot s$ est donc le même que celui des éléments fixés par s, de sorte que $\sigma\cdot s$ est une substitution de même formule que s (on remarquera en effet que, σ étant une bijection de E, les supports, disjoints, des c_i ont pour images les supports des $\sigma\cdot c_i$, qui sont donc disjoints). Réciproquement, deux substitutions de même formule sont conjuguées : en effet, si s et s' sont deux substitutions de même formule, décomposées en cycles non triviaux : $s = c_1 c_2 \ldots c_k$, et $s' = c'_1 c'_2 \ldots c'_k$, où c_i et c'_i ont tous deux pour longueur $\ell_i \geqslant 2$ et s'écrivent :

$$c_i = (\alpha^i_1, \alpha^i_2, \ldots, \alpha^i_{\ell_i})$$

$$c'_i = (\beta^i_1, \beta^i_2, \ldots, \beta^i_{\ell_i})$$

σ devra être tel que : pour tout i $(1 \leqslant i \leqslant k)$:

$$\sigma(\alpha^i_1) = \beta^i_1, \quad \sigma(\alpha^i_2) = \beta^i_2, \quad \ldots, \quad \sigma(\alpha^i_{\ell_i}) = \beta^i_{\ell_i}$$

et dans ce cas on aura : $s' = \sigma\cdot s$.

Lorsque s fixe au moins deux points de E, ou lorsque s contient dans sa décomposition un cycle au moins de longueur paire, on pourra trouver une substitution σ *paire* telle que $s' = \sigma\cdot s$; si σ est impaire, on la compose suivant le cas, soit par une transposition disjointe de s, soit par le cycle de longueur paire contenu dans la décomposition de s, lequel commute avec lui-même et avec tous les autres, donc avec s.

Par suite : Deux substitutions de même formule sont toujours conjuguées, et, sauf peut-être le cas où la formule ne contient que des cycles de longueur impaire et ne fixe qu'un point au plus de E, la conjugaison peut être obtenue au moyen d'une substitution *paire*.

Comme pour le moment nous étudions la conjugaison dans

$\mathcal{S}_n$, cette remarque n'a pas d'intérêt immédiat. Il en résulte de toute façon que, dans le groupe symétrique $\mathcal{S}_n$, toutes les substitutions ayant une même formule appartiennent à la même classe de conjugaison, et celle-ci, de son côté, n'en contient aucune autre. Par suite :

Théorème :

> Chaque classe de conjugaison de $\mathcal{S}_n$ est l'ensemble de toutes les substitutions ayant une même formule $[\ell]$.

Remarque :

Dès lors, le nombre de classes de conjugaison de $\mathcal{S}_n$ est égal au nombre de k-uplets $(\ell_1, \ell_2, \ldots, \ell_k)$, où

$$\ell_1 \geqslant \ell_2 \geqslant \cdots \geqslant \ell_k \geqslant 1$$

$$\ell_1 + \ell_2 + \ldots + \ell_k = n \qquad \text{(d'où } 1 \leqslant k \leqslant n)$$

Une telle suite d'entiers est appelée une "*partition de n*", et le nombre cherché est le nombre de partitions distinctes de l'entier n . On ne connaît malheureusement pas de formule générale donnant en fonction de n le nombre de partitions (distinctes). Pour les premières valeurs de n on a le tableau suivant :

n =	3	4	5	6	7	8	9	10	11	12
Nombre de partitions :	3	5	7	11	15	22	30	40	52	75

Signature d'une substitution de formule donnée :

On sait que la signature d'un cycle de longueur ℓ est $(-1)^{\ell-1}$. Soit s une substitution de formule $[\ell] = (\ell_1, \ell_2, \ldots, \ell_k)$, s est un produit de cycles dont les longueurs sont respectivement les ℓ_i et comme la signature d'un produit de substitutions est égale au produit des signatures, celle de s sera $(-1)^{\ell_1-1}(-1)^{\ell_2-1}\ldots(-1)^{\ell_k-1}$, soit aussi $(-1)^{\ell_1+\ell_2+\ldots+\ell_k-k} = (-1)^{n-k}$.

> La signature d'une substitution de formule $[\ell]$ est égale à $(-1)^{n-k}$, où k est le nombre de cycles entrant dans la composition de la formule $[\ell]$.

Il en résulte que les substitutions paires de $\mathcal{S}_n$ sont celles pour lesquelles la formule présente un nombre de cycles (nombre total, y compris tous les cycles de longueur 1) de même parité que le nombre n d'éléments de E.

b) **Centre de $\mathcal{S}_n$**

Il suffit de rechercher les classes de conjugaison ne contenant qu'un seul élément : il n'en existe de toute évidence qu'une, celle qui correspond à la formule 1^n (donc à l'identité e de l'ensemble E), car il est facile de voir que pour toute autre formule il existe au moins deux substitutions possédant ladite formule. Fait évidemment exception le cas où $n = 2$, dans lequel la formule 2 ne contient qu'une seule substitution qui est la transposition des deux éléments de E. D'ailleurs $\mathcal{S}_2$ est un groupe d'ordre $2! = 2$, qui est abélien puisqu'on a reconnu précédemment qu'un groupe ayant pour ordre un entier premier était abélien.

Théorème :

> Pour $n \geqslant 3$, le centre du groupe symétrique est trivial : $Z(\mathcal{S}_n) = \{e\}$
>
> Pour $n = 2$, le groupe symétrique $\mathcal{S}_2$, d'ordre 2, est abélien, et $Z(\mathcal{S}_2) = \mathcal{S}_2$.

c) **Sous-groupes distingués de $\mathcal{S}_n$**

Nous supposerons d'emblée $n \geqslant 3$, car le résultat est trivial pour $n = 2$, puisque le groupe $\mathcal{S}_2$ n'admet aucun sous-groupe non trivial.

Lemme 1 :

Si un sous-groupe distingué de $\mathcal{S}_n$ contient une transposition, il coïncide avec $\mathcal{S}_n$.

En effet, une transposition est une substitution de formule 2.1^{n-2}, et si un sous-groupe distingué contient une transposition, il les contient toutes, et par suite il contient $\mathcal{S}_n$, puisque le groupe $\mathcal{S}_n$ est engendré par les transpositions. Il en résulte évidemment que ce sous-groupe est égal à $\mathcal{S}_n$, puisqu'à priori il est contenu dans $\mathcal{S}_n$.

Lemme 2 :

Si un sous-groupe distingué de $\mathcal{S}_n$ contient un cycle de longueur 3, il contient le groupe alterné $\mathcal{A}_n$.

En effet, un cycle de longueur 3 a pour formule 3.1^{n-3}, et, si un sous-groupe distingué contient un cycle de longueur 3, il les contient tous, donc il contient $\mathcal{A}_n$, puisque le groupe alterné est engendré par les cycles de longueur 3.

Lemme 3 :

$\mathcal{S}_n$ ne contient aucun sous-groupe propre contenant strictement le groupe alterné $\mathcal{A}_n$.

En effet. si U est un sous-groupe propre (c'est-à-dire non trivial) de $\mathcal{S}_n$, contenant $\mathcal{A}_n$, l'ordre de ce sous-groupe U doit être un diviseur de l'ordre de $\mathcal{S}_n$, soit n ! , et un multiple de celui de $\mathcal{A}_n$, soit $\frac{1}{2}n$! : l'ordre de U doit être un entier de la forme $\frac{k}{2}n$! divisant n ! , ce qui n'est possible que pour les deux valeurs $k = 1$ et $k = 2$. Si $k = 1$, on a : $U = \mathcal{A}_n$, et si $k = 2$, on a : $U = \mathcal{S}_n$, ce qui démontre le lemme.

Remarque :

Le lemme 2 peut alors s'énoncer de façon plus simple :

Si un sous-groupe distingué de $\mathcal{S}_n$ contient un cycle de longueur 3, il coïncide, soit avec $\mathcal{S}_n$, soit avec $\mathcal{A}_n$.

Nous pouvons alors établir, sachant que $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{S}_n$, le théorème fondamental suivant :

Théorème :

Si $n \neq 4$, $\mathcal{S}_n$ ne contient aucun autre sous-groupe distingué non trivial que $\mathcal{A}_n$.

a) Si $n = 3$, les seules formules possibles sont 1^3 , 2.1 et 3 ; si un sous-groupe distingué U est non trivial ($U \neq \mathcal{S}_3$) il ne contient aucune transposition, donc il ne peut contenir, à côté de l'identité (formule 1^3), que des cycles de longueur 3 ; on a donc $U = \mathcal{A}_3$, donc on vérifie bien que c'est un groupe d'ordre 3, et le théorème est ainsi établi dans ce cas.

b) Si $n \geqslant 4$, soit U un sous-groupe distingué non trivial

($U \neq \mathcal{S}_n$) de $\mathcal{S}_n$. Si U contient une transposition (formule 2.1^{n-2}) ou un cycle de longueur 3 (formule 3.1^{n-3}), la réponse est donnée par les lemmes 1 et 2 ; on peut donc supposer ne connaître dans U aucune transposition ni cycle de longueur 3. Soit alors σ un élément de U, qui ne soit ni une transposition, ni un cycle de longueur 3. σ se décompose en un produit de cycles disjoints, selon la formule de σ , et U contient aussi toutes les substitutions de même formule que σ .

1er cas :

La formule de σ contient un cycle de longueur $\ell \geqslant 3$.

On peut prendre pour σ la substitution :

$$\sigma = (1, 2, 3, ..., \ell)\,\tau$$

où τ regroupe les autres cycles de σ ; le support de τ est disjoint de l'ensemble $\{1, 2, ..., \ell\}$. U contient aussi la substitution :

$$\sigma' = (2, 1, 3, ..., \ell)\tau$$

qui a manifestement même formule que σ , et, comme U est un sous-groupe, il contient nécessairement la substitution

$$\sigma'\sigma^{-1} = (2,1,3,....,\ell)\tau\tau^{-1}(1,2,3,....,\ell)^{-1}$$
$$= (2,1,3,....,\ell)(1,2,3,....,\ell)^{-1} = (1,2,3)$$

les autres éléments étant fixés, ainsi qu'on peut le vérifier très facilement (c'est trivial pour les éléments du support de τ ; si i n'est pas un élément de l'ensemble $\{1,2,3\}$, il devient $i-1$ par le cycle $(1,2,3,....,\ell)^{-1}$ et se retransforme en i par le cycle $(2,1,3,....,\ell)$, et enfin 1 devient 2 par l'intermédiaire de ℓ , 2 devient 3 par l'intermédiaire de 1, 3 devient 1 par celui de 2). U contient dans ce cas nécessairement un cycle de longueur 3, et le résultat se trouve dans le lemme 2.

2ème cas :

La formule de σ ne contient que des transpositions, cette formule étant de la forme $2^{\alpha}\cdot 1^{n-2\alpha}$, avec $\alpha \geqslant 2$, sous peine de se retrouver dans le cas trivial du lemme 1. U contient donc toutes les substitutions ayant cette formule, par exemple :

$$\sigma = (1,2)\,(3,4)\tau$$

où τ regroupe les autres cycles et les points fixes de σ .

U contient aussi la substitution :

$$\sigma' = (1,3)\,(2,4)\,\tau$$

qui a manifestement même formule que σ, donc, étant un sous-groupe, U contient également la substitution $\sigma'\sigma^{-1}$ qui s'écrit :

$$\sigma'\sigma^{-1} = (1,3)\,(2,4)\,\tau\tau^{-1}\,(3,4)^{-1}\,(1,2)^{-1} =$$
$$= (1,3)\,(2,4)\,(3,4)\,(1,2)$$

puisque l'inverse d'une transposition est elle-même, et ceci donne :

$$\sigma'\sigma^{-1} = (1,4)\,(2,3)$$

en fixant tous les points du support de τ.

Par suite, U contient dans ce cas toutes les substitutions dont la formule se présente sous la forme $2^2 \cdot 1^{n-4}$.

α) Si $n \geqslant 5$, U contient alors les deux substitutions :

$s = (1,2)\,(3,4)$ fixant tous les autres points,
et $s' = (2,3)\,(4,5)$ fixant tous les autres points,

donc contient aussi $s's^{-1} = (2,3)(4,5)(3,4)(1,2) = (1,3,5,4,2)$, cycle de longueur 5 fixant tous les autres points (s'il en reste), et par suite on se trouve ramené au 1* cas.

Alors le sous-groupe distingué U ne peut être autre que $\mathcal{S}_n$ lui-même (qui est trivial), ou $\mathcal{A}_n$ (il existe un autre sous-groupe distingué trivial, qui est $\{e\}$), ce qui démontre le théorème énoncé.

β) Si $n = 4$, le raisonnement précédent n'est plus valable, et les seules substitutions de formule 2^2 sont

$$s = (1,2)(3,4) \quad , \quad s' = (1,3)(2,4) \quad \text{et} \quad s'' = (1,4)(2,3)$$

qui vérifient $s^2 = s'^2 = s''^2 = 1$, et $ss' = s's = s''$, de sorte qu'avec l'identité e elles constituent un sous-groupe d'ordre 4, bien entendu distingué, appelé le *GROUPE de KLEIN* (Viergruppe) ; une représentation géométrique évidente de ce groupe est donnée par le groupe des symétries par rapport à deux droites perpendiculaires et à leur point d'intersection (géométrie plane).

Il en résulte le théorème suivant :

Théorème :

> Il n'existe dans $\mathcal{S}_4$ que deux sous-groupes distingués non triviaux, qui sont $\mathcal{A}_4$ et le groupe de Klein, d'ordre 4, engendré par les "doubles transpositions".

Les mêmes méthodes vont maintenant nous permettre de traiter le cas du groupe alterné $\mathcal{A}_n$.

IV. ETUDE DE LA STRUCTURE DU GROUPE ALTERNE $\mathcal{A}_n$

Bien que cela ne soit pas strictement indispensable, il est bon de commencer par la détermination des classes de conjugaison dans le groupe alterné $\mathcal{A}_n$, et pour cela de voir au préalable comment $\mathcal{A}_n$ opère par conjugaison sur le groupe symétrique $\mathcal{S}_n$.

On sait que l'ensemble des éléments du groupe symétrique $\mathcal{S}_n$ peut être réparti en *classes*, chaque classe renfermant toutes les substitutions qui ont une formule donnée. Lorsque le groupe $\mathcal{S}_n$ opère par conjugaison sur l'ensemble de ses éléments, il a été démontré que les classes précédentes étaient exactement les classes de conjugaison ; par contre, lorsqu'on fait opérer $\mathcal{A}_n$ (qui est un sous-groupe distingué de $\mathcal{S}_n$) sur l'ensemble des éléments de $\mathcal{S}_n$, les orbites obtenues pourront n'être que des parties de classes — il est sûr en tout cas que la conjuguée par un élément de $\mathcal{A}_n$ d'une substitution est une substitution de même formule, donc appartenant à la même classe.

De fait, compte tenu des remarques faites précédemment (cf. plus haut, III, a, 2*), il est clair que :

Sauf peut-être si la formule de la classe ne contient que des cycles de longueur impaire et fixe au plus un point de l'ensemble E, alors l'orbite d'un élément d'une classe par $\mathcal{A}_n$ est cette classe en entier.

Il en est d'ailleurs de même lorsque la formule d'une classe contient deux cycles de même longueur impaire : si

$$s = (a_1, a_2, \ldots, a_\ell)\,(b_1, b_2, \ldots, b_\ell)t \qquad (\ell \text{ impair})$$

est un élément de cette classe (t fixe chacun des éléments de chacun des deux ensembles disjoints $\{a_1, a_2, \ldots, a_\ell\}$ et $\{b_1, b_2, \ldots, b_\ell\}$). Si s' est une autre substitution de même formule, il existe une substitution $\sigma \in \mathcal{S}_n$ telle que : $s' = \sigma \cdot s$. Si par hasard σ est une substitution impaire, on considère la substitution τ produit de ℓ transpositions disjointes :

$$\tau = (a_1, b_1)\,(a_2, b_2)\,\ldots\,(a_\ell\, b_\ell)\,,$$

manifestement impaire (puisque ℓ est impair), et commutant avec s puisque :

$$\tau \cdot s = (b_1, b_2, \ldots, b_\ell)(a_1, a_2, \ldots, a_\ell)t = s \ ,$$

τ commute avec t puisque leurs supports sont disjoints, et les deux cycles commutent, étant disjoints. Il en résulte que : $s' = \sigma \cdot s = \sigma \cdot (\tau \cdot s) = (\sigma\tau) \cdot s$ avec une substitution $\sigma\tau$ paire : dans ce cas deux éléments quelconques de cette classe sont conjugués, et on peut toujours s'arranger pour obtenir une substitution paire, de sorte que la classe entière constitue une orbite pour l'opération de $\mathcal{A}_n$.

Il ne reste plus qu'à étudier le cas des classes ne contenant que des cycles de *longueurs impaires distinctes* (ce qui entraîne ipso facto la fixation d'un point de E au plus, puisque le nombre de cycles de longueur 1 est égal au plus à 1).

Soit $\mathcal{C}$ une classe quelconque (au sens qui est donné ci-dessus à ce vocable) ; considérons deux éléments s et s' de cette classe $\mathcal{C}$, choisis de telle sorte qu'il existe une substitution σ *impaire* telle que $s' = \sigma \cdot s$ (il existe toujours au moins une substitution ayant cette propriété, mais elle peut être paire ou impaire), et les orbites $\gamma(s)$ et $\gamma(s')$ de ces deux éléments respectifs dans l'opération de conjugaison de $\mathcal{C}$ par les éléments de $\mathcal{A}_n$.

a) On a tout d'abord : $\mathcal{C} = \gamma(s) \cup \gamma(s')$, car tout élément t pris dans $\mathcal{C}$ est le conjugué de s par une substitution τ : $t = \tau \cdot s$. Ou bien τ est paire, et alors t appartient à $\gamma(s)$; ou bien τ est impaire, et il existe une substitution τ' paire telle que $\tau = \tau'\sigma$: alors :
$t = \tau \cdot s = (\tau'\sigma) \cdot s = \tau' \cdot (\sigma \cdot s) = \tau' \cdot s'$, et dans ce cas t est un élément de $\gamma(s')$.

b) Il existe une bijection naturelle entre $\gamma(s)$ et $\gamma(s')$, car, si t est un élément de $\gamma(s)$, il existe une substitution paire $x \in \mathcal{A}_n$ telle que $t = x \cdot s$, et on peut lui associer bijectivement l'élément t' de $\gamma(s')$ défini par :

$$t' = \sigma \cdot t = \sigma \cdot (x \cdot s) = (\sigma x) \cdot s = (\sigma x \sigma^{-1} \sigma) \cdot s$$
$$= (x^{\sigma^{-1}} \sigma) \cdot s = x^{\sigma^{-1}} \cdot (\sigma \cdot s) = x^{\sigma^{-1}} \cdot s' = y \cdot s'$$

où $y = x^{\sigma^{-1}}$ est bien un élément de $\mathcal{A}_n$, puisque x en est un et que $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{S}_n$.

Il s'ensuit, puisqu'on a affaire à des ensembles finis, que $\gamma(s)$ et $\gamma(s')$ ont le même nombre d'éléments.

c) Par suite, seules deux configurations sont possibles :
— ou bien $\gamma(s) = \gamma(s') = \mathcal{C}$, et alors $\mathcal{C}$ entier constitue une orbite : on a vu que cette configuration était la plus fréquente ;
— ou bien $\gamma(s) \cap \gamma(s') = \phi$, et alors $\mathcal{C}$ se partage en exactement deux orbites ayant le même nombre d'éléments.

d) En fait, la deuxième de ces configurations arrive nécessairement dans le cas d'une classe $\mathcal{C}$ dont la formule ne contient que des cycles de longueurs impaires distinctes. Il suffit pour cela d'établir que seules des substitutions paires peuvent commuter avec un élément donné s de cette classe : en effet, si s et s' sont deux éléments de $\mathcal{C}$ tels que $s' = \sigma \cdot s$, où σ est une substitution impaire, on aura $\gamma(s) = \gamma(s')$ si et seulement si s' est un élément de $\gamma(s)$, c'est-à-dire s'il existe une substitution paire τ telle que $s' = \tau \cdot s$, ce qui entraîne $\tau \cdot s = \sigma \cdot s$, soit $(\sigma^{-1}\tau) \cdot s = s$, donc $\sigma^{-1}\tau$, qui est impaire, commute avec s ; si réciproquement il existe une substitution impaire τ' commutant avec s , alors $\tau' \cdot s = s$, et $s' = \sigma \cdot s = (\sigma\tau') \cdot s$, et puisque $\sigma\tau'$ est paire, s' est un élément de $\gamma(s)$, et alors $\gamma(s) = \gamma(s') = \mathcal{C}$. Ceci montre bien qu'inversement, on aura la deuxième configuration si et seulement si seules des substitutions paires commutent avec s .

e) Il reste à mettre en oeuvre cette recherche dans les hypothèses indiquées en d) ; si s est décomposé en cycles : $s = c_1 c_2 \ldots c_k$ de façon *unique*, le cycle c_i ayant pour longueur ℓ_i impaire, et $\ell_1 > \ell_2 > \ldots > \ell_k \geqslant 1$. Pour une substitution σ quelconque, on a ainsi qu'il a été vu : $\sigma \cdot s = (\sigma \cdot c_1)(\sigma \cdot c_2) \ldots (\sigma \cdot c_k)$, qui est un élément appartenant aussi à $\mathcal{C}$, et où donc $\sigma \cdot c_i$ est un cycle de longueur ℓ_i ; de $\sigma \cdot s = s$, puisque par hypothèse σ commute avec s , on tire d'après l'unicité de la décomposition en cycles que $\sigma \cdot c_i = c_i$ et que par conséquent σ conserve le support de chacun des cycles composant s . Il suffit donc de considérer les k substitutions $\sigma_1, \sigma_2, \ldots, \sigma_k$, où σ_i coïncide sur le support du cycle c_i avec la restriction de σ, et fixe les autres points de E : dans ces conditions, il est clair que $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$; les σ_i commutent deux à deux puisqu'ils ont des supports disjoints.

On est ramené, sur un ensemble de ℓ éléments, à trouver quelles substitutions commutent avec un cycle de longueur ℓ.

Numérotant les éléments de E de telle sorte que ce cycle soit : $c = (1, 2, 3, \ldots, \ell)$, alors $\sigma \cdot c$ est le cycle $(\sigma(1), \sigma(2), \ldots, \sigma(\ell))$, et on aura $\sigma \cdot c = c$ si et seulement si

$c[\sigma(1)] = \sigma(1) + 1 = \sigma(2)$. Posant $\sigma(1) = \alpha$, on devra avoir $\sigma(2) = \alpha + 1, \ldots$ etc, de sorte que σ n'est autre que le cycle c^{α}.

En revenant au problème posé, on voit que les substitutions σ qui commutent avec $s = c_1 c_2 \ldots c_k$, où les c_i sont des cycles disjoints de longueurs ℓ_i inégales ($\ell_1 \neq \ell_2 \neq \ldots \neq \ell_k$), sont toutes les substitutions qui s'écrivent $\sigma = c_1^{\alpha_1} c_2^{\alpha_2} \ldots c_k^{\alpha_k}$ où α_i est un entier tel que $1 \leqslant \alpha_i \leqslant \ell_i$. Les longueurs des cycles composants étant toutes impaires, tous les cycles c_i sont des substitutions paires, et il en est donc de même de σ.

a) **Conjugaison dans $\mathcal{A}_n$**

On recherche ici quelles sont les classes de conjugaison de $\mathcal{A}_n$.

Pour obtenir les éléments de $\mathcal{A}_n$ on ne conserve que les classes $\mathcal{C}$ dans lesquelles la formule présente un nombre total de cycles (y compris les cycles de longueur 1) qui a la même parité que n.

Alors, d'après ce qui précède, les classes de conjugaison de $\mathcal{A}_n$ sont, sauf le cas d'exception de celles dont la formule révèle uniquement des cycles de longueurs impaires et distinctes, et qui se partagent en deux classes de conjugaison ayant le même nombre d'éléments, des classes $\mathcal{C}$ dont il vient d'être question.

En particulier, si $n \geqslant 5$ les cycles de longueur 3 forment une seule classe de conjugaison, puisque leur formule est $3 \cdot 1^{n-3}$, avec $n - 3 \geqslant 2$; par suite tout sous-groupe distingué de $\mathcal{A}_n$ qui contient un cycle de longueur 3 les contient tous, et donc coïncide avec $\mathcal{A}_n$ (puisque de toute façon ce sous-groupe est contenu dans $\mathcal{A}_n$).

Par contre, une étude spéciale sera nécessaire dans les cas $n = 3$ et $n = 4$: dans ce dernier cas en particulier les cycles de longueur 3 répondent à la formule $3 \cdot 1$ et ils se répartissent en deux classes de conjugaison contenant le même nombre d'éléments.

b) **Sous-groupes distingués de $\mathcal{A}_n$**

$\boxed{n \geqslant 5}$

Un sous-groupe distingué de $\mathcal{A}_n$ qui contient un cycle de longueur 3 coïncide avec $\mathcal{A}_n$ (voir plus haut).

Soit alors U un sous-groupe distingué de $\mathcal{A}_n$: si σ est un élément de U, alors U contient en entier la classe de conjugaison de σ.

1er cas : σ contient un cycle de longueur $\ell \geqslant 4$.

Il nous est loisible de ranger les éléments de E dans un ordre tel que cet élément soit : $\sigma = (1,2,3,4,\ldots,\ell)\tau$.

Un autre élément de la classe de conjugaison de σ est $s \cdot \sigma$, où $s = (1,2,3)$, cycle de longueur 3 fixant les autres éléments, et donc commutant avec τ, de sorte que :

$$s \cdot \sigma = \sigma' = (2,3,1,4, \ldots, \ell)\tau$$

et σ' est aussi un élément de U. U contient par suite l'élément :

$$\begin{aligned} \sigma'\sigma^{-1} &= (2,3,1,4, \ldots, \ell)\tau\tau^{-1} (1,2,3,4, \ldots \ell)^{-1} \\ &= (2,3,1,4, \ldots, \ell)(1,2,3,4, \ldots, \ell)^{-1} = (1,2,4), \end{aligned}$$

qui est un cycle de longueur 3. D'après le lemme 2 (voir II, c), on a donc $U = \mathcal{A}_n$.

2ème cas : σ contient au moins un cycle de longueur 3. On supposera évidemment que σ n'est pas un cycle de longueur 3 (sinon le cas serait trivial et on aurait $U = \mathcal{A}_n$) et donc qu'il existe également dans la décomposition de σ un autre cycle de longueur 2 ou 3 (il est inutile, sous peine de retomber dans le premier cas étudié, de considérer le cas où ce cycle aurait une longueur au moins égale à 4). Moyennant une numérotation convenable des éléments de l'ensemble E, σ pourra s'écrire : $\sigma = (1,2,3)(4,5,\ell)\tau$ où $\ell = 5$ ou 6 (dans le cas $\ell = 5$ le deuxième cycle se réduit à la transposition (4,5)), et U contient toutes les substitutions de la forme $s \cdot \sigma$, avec $s \in \mathcal{A}_n$. Si on prend $s = (1,2)(3,4)$ (les autres points étant fixés par s), on a : $\sigma' = s \cdot \sigma = (2,1,4)(3,5,\ell)\tau$ car s étant disjoint de τ commute avec τ ; d'autre part, si $\ell = 5$ le deuxième cycle se réduit à la transposition (3,5). U contenant σ et σ' contient aussi $\sigma'\sigma^{-1}$, soit :

$$(2,1,4)(3,5,\ell)\tau\tau^{-1} (4,5,\ell)^{-1} (1,2,3)^{-1}, \text{ soit encore :}$$

$(2,1,4)(3,5,\ell)(4,\ell,5)(1,3,2) = (1,5,2,4,3)(\ell)$, et les autres points sont fixés ; lorsque $\ell = 5$, on vérifie facilement que le résultat reste valable car :

$\sigma'\sigma^{-1} = (2,1,4)(3,5)(4,5)(1,3,2) = (1,5,2,4,3)$, les autres points de E étant fixés.

Il s'ensuit que U contient un cycle de longueur 5, ce qui ramène, par application du résultat trouvé dans le premier cas, à la même conclusion, c'est-à-dire $U = \mathcal{A}_n$.

3ème cas : σ ne contient que des cycles de longueur 2 (évidemment en nombre pair). Puisque $n \geqslant 5$, on peut moyennant un ordre convenable de numérotation des éléments de E supposer que :

$\sigma = (1,2)(3,4)\tau$, où τ regroupe les autres cycles de σ.

U étant distingué contient aussi $\sigma' = s\cdot\sigma$, pour toute substitution paire s, en particulier pour $s = (1,2,3)$, cycle de longueur 3 fixant les autres points de E, et commutant avec τ puisque disjoint de τ. Alors : $\sigma' = (2,3)(1,4)\tau$, et par suite U contenant σ et σ' contient aussi

$$\sigma'\sigma^{-1} = (2,3)(1,4)\tau\tau^{-1}(3,4)^{-1}(1,2)^{-1} = (2,3)(1,4)(3,4)(1,2)$$

compte tenu du fait qu'une transposition est sa propre inverse, les autres points étant fixés par $\sigma'\sigma^{-1} = (1,3)(2,4)$.

U contient donc un produit de deux transpositions, dont la formule est $2^2\cdot 1^{n-4}$ et dont la classe de conjugaison est composée (dans $\mathcal{A}_n$) de *toutes* les substitutions ayant cette formule.

U contient donc par exemple les deux substitutions :

$$\sigma = (1,2)(3,4) \qquad \text{et} \qquad \tau = (1,2)(3,5)$$

(chacune fixant les autres points), donc aussi leur produit $\sigma\tau = (1,2)(3,4)(1,2)(3,5) = (3,5,4)$, c'est-à-dire un cycle de longueur 3.

Comme $n \geqslant 5$, un cycle de longueur 3 fixe au moins deux points, et par suite la classe de conjugaison (dans $\mathcal{A}_n$) d'un cycle de longueur 3 est constituée par l'ensemble de tous les cycles de longueur 3 : ainsi qu'il a été vu, on a nécessairement $U = \mathcal{A}_n$.

Théorème :

> Lorsque $n \geqslant 5$, le groupe alterné $\mathcal{A}_n$ ne contient aucun sous-groupe distingué non trivial.

Autrement dit : $\mathcal{A}_n$ est un *groupe simple*.

On étudie maintenant les deux cas particuliers où $n = 3$ ou 4.

n = 3

Alors l'ordre de $\mathcal{S}_3$ est $3\,! = 6$, et celui de $\mathcal{A}_3$ est égal à 3. $\mathcal{A}_3$ est alors un groupe dont l'ordre est un entier premier, il est donc abélien (et même cyclique) et ne possède aucun sous-groupe non trivial — on remarque que dans un groupe abélien tout sous-groupe est distingué. Le théorème ci-dessus est donc encore vrai dans le cas où $n = 3$.

n = 4

Ce cas a déjà été entrevu lors de l'étude des sous-groupes distingués du groupe symétrique $\mathcal{S}_4$, ces sous-groupes étant, outre le groupe alterné $\mathcal{A}_4$, un sous-groupe V (groupe de Klein) formé de l'identité et des trois substitutions de formule 2^2 (produits de deux transpositions disjointes), donc paires, de sorte que ce sous-groupe V est contenu dans $\mathcal{A}_4$. $\mathcal{A}_4$ possède donc un sous-groupe distingué non trivial V, et on se convaincra aisément qu'il n'en existe pas d'autre. En effet, les éléments de $\mathcal{S}_4$ se répartissent en cinq classes répondant aux formules respectives :

$$4\ ,\ 3\cdot 1\ ,\ 2^2\ ,\ 2\cdot 1^2 \quad \text{et} \quad 1^4$$

et ceux de $\mathcal{A}_4$ en les trois classes de substitutions paires (le nombre k des cycles devant être de même parité que n, ici doit être pair puisque $n = 4$), soient les classes $3\cdot 1$, 2^2 et 1^4 : dans $\mathcal{A}_4$ on trouve alors les classes de conjugaison suivantes :

— les classes de formules 1^4 et 2^2 forment chacune une classe de conjugaison de $\mathcal{A}_4$, la première ne contenant que l'élément neutre et la deuxième que les trois substitutions produits de deux transpositions disjointes ; leur réunion constitue le sous-groupe distingué V déjà connu et par suite il n'existe aucun sous-groupe distingué de $\mathcal{A}_4$ contenu dans V ;

— la classe de formule $3\cdot 1$ contenant tous les cycles de longueur 3 se subdivise en deux classes de conjugaison de $\mathcal{A}_4$.

Si U est un sous-groupe distingué de $\mathcal{A}_4$ distinct de V et de $\{e\}$, il contient au moins un cycle σ de longueur 3, ainsi que son inverse σ^{-1} : il contient donc la réunion des classes de conjugaison de ces éléments σ et σ^{-1} ; or ces deux éléments sont situés dans

deux classes de conjugaison distinctes car, moyennant une numérotation convenable des éléments de E, on peut écrire $\sigma = (1,2,3)(4)$, d'où $\sigma^{-1} = (1,3,2)(4)$, et une substitution τ telle que $\sigma^{-1} = \tau \cdot \sigma$ est la transposition (2,3) fixant 1 et 4, donc une substitution impaire. Dans ces conditions U contient nécessairement *tous* les cycles de longueur 3, et par suite il coïncide avec $\mathcal{A}_4$.

Théorème :

> Le groupe alterné $\mathcal{A}_4$ ne contient qu'un seul sous-groupe distingué non trivial qui est le groupe de Klein engendré par les "doubles transpositions".

En regroupant ces résultats et tenant compte qu'il suffit de remarquer que le groupe alterné $\mathcal{A}_2$ se réduit à $\{e\}$, on obtient le théorème général suivant :

Théorème :

> Le groupe alterné $\mathcal{A}_n$ est *simple* lorsque $n \neq 4$.

c) **Centre de $\mathcal{A}_n$**

De ce qui précède on peut déduire quel est le centre de $\mathcal{A}_n$, qui est $\mathcal{A}_n$ tout entier lorsque celui-ci est abélien (cas $n = 2$ et $n = 3$) et qui dans le cas contraire est un sous-groupe distingué autre que $\mathcal{A}_n$: il est donc assuré que $Z(\mathcal{A}_n) = \{e\}$ dans tous les cas où $n \geqslant 5$. Il reste à examiner directement le cas où $n = 4$, mais on s'assure directement que le sous-groupe distingué V n'est pas le centre puisqu'il n'est pas composé uniquement de classes de conjugaison ne renfermant qu'un seul élément. Il en résulte alors :

Théorème :

> Pour $n \geqslant 4$, le centre du groupe alterné est trivial :
> $$Z(\mathcal{A}_n) = \{e\}$$
> Pour $n = 2$ et $n = 3$, le groupe alterné $\mathcal{A}_n$ est abélien, et
> $$Z(\mathcal{A}_2) = \mathcal{A}_2 \quad , \quad Z(\mathcal{A}_3) = \mathcal{A}_3$$

En guise de conclusion ...

Ces théorèmes de structure sont très importants et à la base de la théorie des équations algébriques. En particulier, le fait que le groupe alterné $\mathcal{A}_n$ est simple pour $n \geqslant 5$ constitue la raison fondamentale (bien que n'apparaissant pas explicitement dans les premières démonstrations de ce fait) de l'impossibilité de résoudre par radicaux l'équation algébrique générale dont le degré est au moins égal à 5, alors que cela est possible pour le degré 4 (le résultat est bien connu depuis longtemps dans le cas des degrés 2 et 3).

Sans prétendre donner de cette propriété une démonstration complète qui mettrait en oeuvre la théorie de GALOIS (sur les extensions de corps), il est possible de donner une idée du raisonnement. On considère une équation algébrique de degré n, s'écrivant $P(x) = 0$, où P est un polynôme de degré n qui dépend de n coefficients — le coefficient dominant pouvant toujours être supposé égal à 1. Si F est le plus petit sous-corps du corps des complexes contenant tous les coefficients de P (F est un corps contenant le corps Q des rationnels, et pour les polynômes usuellement utilisés il se réduit le plus souvent à Q), P est un polynôme à coefficients dans F, en général irréductible et par conséquent on peut de proche en proche construire le corps de rupture F_P de ce polynôme ; ce corps est la plus petite extension de F qui contienne toutes les racines de P. La théorie de Galois montre alors qu'il existe un groupe d'automorphismes du corps F_P, laissant fixes les éléments du corps F, et dont l'effet est de permuter les zéros du polynôme P, qui ont été progressivement adjoints lors de la construction. Ce groupe, appelé le GROUPE DE GALOIS de l'équation, est donc en général un sous-groupe du groupe symétrique $\mathcal{S}_n$ (puisqu'il y a n racines à une équation de degré n) ; il peut être $\mathcal{S}_n$ exactement (c'est le cas général) mais il peut aussi être plus petit, pour des formes particulières d'équations (par exemple dans le cas d'équations réciproques).

Si on appelle G le groupe de Galois du polynôme P, et si l'on considère un stade intermédiaire où des racines ont été isolées, mais où il reste un facteur irréductible P', alors $F_P = F'_P$, est le corps de rupture du polynôme P' par rapport au corps intermédiaire F', et il existe un groupe de Galois G' qui est un sous-groupe distingué de G tel que le groupe-quotient G/G' soit le groupe de Galois de l'extension F' par rapport à F. Or on conçoit bien intui-

tivement qu'un élément de F′ pourra s'exprimer à partir d'éléments de F au moyen d'un radical k-ième seulement si ce groupe de Galois G/G′ est lui-même cyclique d'ordre k (ou un multiple de k). Par suite on conçoit fort bien qu'une condition pour que les racines de l'équation $P(x) = 0$ puissent s'exprimer au moyen des coefficients avec des radicaux doive être que le groupe G possède une suite de sous-groupes emboîtés :

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_{k-1} \supset G_k = \{1\}$$

tels que chacun d'eux soit un sous-groupe distingué du précédent et qu'en outre chaque groupe-quotient G_i/G_{i+1} soit cyclique (on dit alors que le groupe G est résoluble).

Or, pour l'équation générale de degré n, $G = \mathcal{S}_n$, et, $\mathcal{A}_n$ étant simple pour $n \geqslant 5$, la seule suite possible de sous-groupes dans ce cas est :

$$\mathcal{S}_n \supset \mathcal{A}_n \supset \{e\} .$$

Si $\mathcal{S}_n / \mathcal{A}_n$ est bien cyclique d'ordre 2, il n'en est pas de même de $\mathcal{A}_n$, qui n'est même pas abélien ...

Pour $n = 4$, il existe la suite $\mathcal{S}_4 \supset \mathcal{A}_4 \supset V \supset H \supset \{e\}$ où H est un sous-groupe d'ordre 2 de V (nécessairement distingué dans V car V est abélien), et, les ordres de ces groupes étant respectivement 24, 12, 4 et 2, les groupes-quotients successifs sont :

$\mathcal{S}_4 / \mathcal{A}_4$, cyclique d'ordre 2, $\mathcal{A}_4$/V, cyclique d'ordre 3, V/H, cyclique d'ordre 2 et enfin H, cyclique d'ordre 2.

Le groupe $\mathcal{S}_4$ étant résoluble, l'équation générale du quatrième degré est résoluble par radicaux, et toute racine pourra s'exprimer en fonction des coefficients par une formule ne mettant en oeuvre que des radicaux carrés et des radicaux cubiques.

Pour $n = 3$, le résultat est encore plus évident car la chaîne de sous-groupes utilisée est $\mathcal{S}_3 \supset \mathcal{A}_3 \supset \{e\}$, et les groupes-quotients sont cycliques, l'un d'ordre 2 et l'autre d'ordre 3, ce qui explique que les formules classiques de résolution du troisième degré (formule de Cardan par exemple) mettent en oeuvre elles aussi des radicaux carrés et des radicaux cubiques.

APPENDICE :

STRUCTURE DU GROUPE $0^+(\mathbf{R}^3)$ DES ROTATIONS VECTORIELLES DE L'ESPACE EUCLIDIEN DE DIMENSION 3

La méthode utilisée pour trouver les sous-groupes distingués d'un groupe est générale ; lorsque le groupe possède une signification géométrique — comme c'est le cas pour le groupe symétrique et le groupe alterné — la recherche des classes de conjugaison est parfois relativement facile. A titre de complément à cette étude, et bien que le groupe envisagé ne soit pas un groupe fini et n'ait aucun lien avec ce qui précède, il est intéressant de voir comment les méthodes précédentes s'utilisent pour démontrer la simplicité d'un groupe remarquable, le groupe $0^+(\mathbf{R}^3)$ des rotations vectorielles de l'espace euclidien ordinaire à trois dimensions.

Une rotation vectorielle de l'espace $\mathbf{R}^3$ est caractérisée par la donnée d'un vecteur unitaire $\vec{\omega}$ (c'est-à-dire de norme euclidienne égale à 1) et d'un angle de rotation, représenté par un nombre réel θ tel que $0 \leqslant \theta \leqslant \pi$; une rotation d'angle π est un demi-tour, et les demi-tours représentés par $(\vec{\omega}, \pi)$ et $(-\vec{\omega}, \pi)$ sont identiques ; on peut d'ailleurs dire qu'en dehors de ce cas la représentation d'une rotation autre que l'identité par $(\vec{\omega}, \theta)$ est unique. On sait par ailleurs que toute rotation est décomposable en le produit de deux demi-tours, de sorte que le groupe $0^+(\mathbf{R}^3)$ est *engendré* par les demi-tours.

Soit $\rho(\vec{\omega}, \theta)$ une rotation ; si σ est un élément quelconque de $0^+(\mathbf{R}^3)$, c'est-à-dire en fait une rotation, le conjugué de ρ par σ^{-1} est la rotation $\rho' = \sigma \circ \rho \circ \sigma^{-1}$, et il est clair que, pour tout vecteur $\vec{v}$ de $\mathbf{R}^3$, on a : $\rho'[\sigma(\vec{v})] = \sigma[\rho(\vec{v})]$, de sorte que, en prenant pour $\vec{v}$:

— le vecteur $\vec{\omega}$ tel que $\rho(\vec{\omega}) = \vec{\omega}$, on trouve $\rho'[\sigma(\vec{\omega})] = \sigma(\vec{\omega})$, et par suite l'axe de la rotation ρ' est déterminé par le vecteur unitaire $\sigma(\vec{\omega})$;

— un vecteur unitaire orthogonal à $\vec{\omega}$, on a : $\vec{v} \cdot \rho(\vec{v}) = \cos\theta$, et de plus, σ étant une rotation, $\sigma(\vec{v})$ est orthogonal à $\sigma(\vec{\omega})$, et on a :

$$\sigma(\vec{v}) \cdot \rho'[\sigma(\vec{v})] = \sigma(\vec{v}) \cdot \sigma[\rho(\vec{v})] = \vec{v} \cdot \rho(\vec{v}) = \cos\theta$$

puisque σ, étant une rotation, conserve la valeur du produit scalaire, et il en résulte que l'angle de ρ' est θ.

Par suite, ρ' est la rotation $(\sigma(\vec{\omega}), \theta)$.

Réciproquement, soient $\rho\ (\vec{\omega},\theta)$ et $\rho'\ (\vec{\omega}',\theta)$ deux rotations vectorielles de même angle : elles sont certainement conjuguées dans le groupe $0^+(\mathbf{R}^3)$, et $\rho' = \rho^{\sigma^{-1}}$ si σ est l'une quelconque des rotations vectorielles de $\mathbf{R}^3$ qui transforment $\vec{\omega}$ en $\vec{\omega}'$, d'où il résulte qu'à chaque angle θ $(0 \leqslant \theta \leqslant \pi)$ correspond une classe de conjugaison qui contient *toutes* les rotations d'angle θ. On note que, dans le cas où $\theta = 0$, la classe de conjugaison correspondante ne contient qu'un seul élément, qui est l'identité. Lorsque $\theta = \pi$ on obtient aussi une classe de conjugaison qui contient *tous* les demi-tours, de sorte que :

Lemme :

> Si un sous-groupe distingué de $0^+(\mathbf{R}^3)$ contient un demi-tour, il coïncide nécessairement avec $0^+(\mathbf{R}^3)$.

Remarque :

Si ρ est la rotation $(\vec{\omega}, \theta)$, la rotation réciproque ρ^{-1} représentée par $(-\vec{\omega}, \theta)$ appartient toujours à la même classe de conjugaison que ρ.

Nous pouvons alors rechercher les sous-groupes distingués non triviaux de $0^+(\mathbf{R}^3)$; soit N l'un d'eux, $\rho(\vec{\omega}, \theta)$ un élément de N. On suppose évidemment $\theta \neq 0$, sinon ρ serait l'identité, et $\theta \neq \pi$, sinon ρ serait un demi-tour, et l'application du lemme donnerait immédiatement $N = 0^+(\mathbf{R}^3)$. Si $\theta = \frac{\pi}{2}$, N contient aussi ρ^2 qui est la rotation $(\vec{\omega}, 2\theta) = (\vec{\omega}, \pi)$ qui est un demi-tour, qui ramène au cas du lemme.

On peut toujours supposer $\frac{\pi}{2} < \theta < \pi$: en effet, s'il n'en était pas ainsi on aurait, hormis les cas triviaux précédents, $0 < \theta < \frac{\pi}{2}$; et il existe dans ce cas un entier $k > 0$ tel que $\frac{\pi}{2^{k+1}} < \theta \leqslant \frac{\pi}{2^k}$, de sorte que $\frac{\pi}{2} < 2^k\theta \leqslant \pi$, et N contenant ρ contient aussi la rotation ρ^{2^k} qui a précisément pour angle $\theta' = 2^k\theta$, avec $\frac{\pi}{2} < \theta' \leqslant \pi$; le cas où $\theta' = \pi$ donne pour ρ^{2^k} un demi-tour qui ramène au cas du lemme. Hormis les cas triviaux il est donc toujours possible de supposer que N contient une rotation ρ d'axe déterminé par $\vec{\omega}$ et dont l'angle θ satisfait à : $\frac{\pi}{2} < \theta < \pi$.

N contenant une rotation ρ ayant pour angle θ les contient toutes, puisque N est un sous-groupe distingué ; s'il contient deux rotations ρ et ρ', il contient leur produit $\rho \circ \rho'$, et il est facile de trouver deux rotations dont le même angle θ satisfait à la condition précédente, dont le produit soit un demi-tour :

Si D et D′ sont deux droites vectorielles dont l'un des angles a pour mesure $\frac{\theta}{2}$ (avec $\frac{\pi}{4} < \frac{\theta}{2} < \frac{\pi}{2}$, compte tenu de l'hypothèse faite sur θ) le produit $\rho = d' \circ d$ des demi-tours d et d′ d'axes respectifs D et D′ est une rotation d'angle θ, donc un élément de N ; il en est de même de $\rho' = d \circ d''$, où d et d″ sont les demi-tours d'axes les droites vectorielles D et D″, D″ étant choisie telle que l'un des angles des droites D et D″ ait aussi pour mesure $\frac{\theta}{2}$. Alors on aura : $\rho \circ \rho' = d' \circ d''$ sera le produit des rotations vectorielles d″ et d′ d'axes D″ et D′, et ce sera aussi un élément de N. Or, $\rho \circ \rho'$ est lui-même un demi-tour si et seulement si les droites vectorielles D′ et D″ sont orthogonales. Un raisonnement simple, soit géométrique, soit analytique en se rapportant à un repère orthonormé bien choisi, montre que, sous réserve que l'inégalité $\frac{\pi}{2} < \theta < \pi$ soit satisfaite, il existe, D et D′ étant données, deux droites D″ satisfaisant à cette condition, ce qui est d'ailleurs plus que suffisant pour montrer que N contient un demi-tour.

La conclusion est que tout sous-groupe distingué de $0^+(\mathbf{R}^3)$ distinct de { Identité } coïncide avec $0^+(\mathbf{R}^3)$, et par suite que :

Théorème :

> $0^+(\mathbf{R}^3)$ ne contient aucun sous-groupe distingué non trivial.

Autrement dit, on obtient là une propriété remarquable du groupe $0^+(\mathbf{R}^3)$ des rotations vectorielles de l'espace euclidien ordinaire de dimension 3 :

> Le groupe $0^+(\mathbf{R}^3)$ des rotations vectorielles de l'espace euclidien ordinaire de dimension 3 est *simple*.

Remarque :

Plusieurs représentations algébriques de ce groupe existent, et on peut tout d'abord noter que, dans le cas de l'espace vectoriel $\mathbf{R}^3$ des vecteurs de l'espace ordinaire, muni de sa structure euclidienne habituelle et du produit vectoriel, l'image $\rho(\vec{v})$ d'un vecteur

arbitraire $\vec{v}$ de cet espace par la rotation $\rho\,(\vec{\omega}, \theta)$ (avec $0 \leqslant \theta \leqslant \pi$) est donnée par l'expression :

$$\rho(\vec{v}) = \vec{v}\cos\theta + (\vec{\omega} \wedge \vec{v})\sin\theta + 2\sin^2\frac{\theta}{2}\,(\vec{\omega}\cdot\vec{v})\vec{\omega}$$

qui confère à l'ensemble $S^2 \times [0, \pi]$ (où S^2 est la "sphère de rayon 1", c'est-à-dire l'ensemble des vecteurs de $\mathbf{R}^3$ ayant pour norme 1) une structure de groupe isomorphe à $0^+(\mathbf{R}^3)$; malheureusement son emploi est très malaisé et il vaut mieux représenter ce groupe comme groupe de matrices :

— soit classiquement comme matrices orthogonales de $\mathbf{R}^3$, dont la forme canonique est :

$$M = \begin{pmatrix} \alpha^2-\beta^2-\gamma^2+\delta^2 & 2(\alpha\beta-\gamma\delta) & 2(\alpha\gamma+\beta\delta) \\ 2(\alpha\beta+\gamma\delta) & -\alpha^2+\beta^2-\gamma^2+\delta^2 & 2(\beta\gamma-\alpha\delta) \\ 2(\alpha\gamma-\beta\delta) & 2(\beta\gamma+\alpha\delta) & -\alpha^2-\beta^2+\gamma^2+\delta^2 \end{pmatrix}$$

dans laquelle $\alpha, \beta, \gamma, \delta$ sont quatre nombres réels satisfaisant à la relation : $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$. Cette matrice se réduit à la matrice unité lorsque $|\delta| = 1$; comme d'autre part $|\delta| \leqslant 1$ en vertu de la condition précédente, et que M ne change pas quand on y remplace simultanément $\alpha, \beta, \gamma, \delta$ par $-\alpha, -\beta, -\gamma, -\delta$ respectivement, il nous est toujours loisible de supposer $\delta \geqslant 0$ et, par suite, les nombres réels $\alpha, \beta, \gamma, \delta$ étant assujettis aux relations :

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1 \quad \text{avec} \quad 0 \leqslant \delta < 1$$

(le cas $\delta = 1$ donnant alors l'identité), la matrice M représente, dans une base orthonormée de $\mathbf{R}^3$, une rotation $\rho\,(\vec{\omega}, \theta)$, de façon unique, par les identifications suivantes : si les composantes de $\vec{\omega}$ sont (p, q, r) avec $p^2 + q^2 + r^2 = 1$, alors :

$\alpha = p\sin\frac{\theta}{2}$, $\beta = q\sin\frac{\theta}{2}$, $\gamma = r\sin\frac{\theta}{2}$ et $\delta = \cos\frac{\theta}{2}$ (on a supposé $0 < \theta \leqslant \pi$) ;

— soit au moyen des quaternions de norme 1, dont l'interprétation géométrique est loin d'être immédiate, pouvant eux-mêmes être représentés de deux manières équivalentes :

— ou bien par la matrice suivante, utilisant les mêmes notations et identifications que dans la représentation matricielle classique précédente :

$$H = \begin{pmatrix} \delta & \alpha & \beta & \gamma \\ -\alpha & \delta & -\gamma & \beta \\ -\beta & \gamma & \delta & -\alpha \\ -\gamma & -\beta & \alpha & \delta \end{pmatrix}$$

un vecteur $\vec{v}$ de $\mathbf{R}^3$ étant alors représenté dans le repère orthonormé choisi, dans lequel ses composantes sont (x, y, z), par la matrice :

$$V = \begin{pmatrix} 0 & x & y & z \\ -x & 0 & -z & y \\ -y & z & 0 & -x \\ -z & -y & x & 0 \end{pmatrix}$$

la matrice représentant le vecteur $\rho(\vec{v})$ est alors $V' = H\,V\,{}^tH$, où ${}^tH$ représente la matrice transposée de H, le produit écrit étant un produit ordinaire de matrices ; on remarque d'ailleurs que la matrice H est elle-même une matrice orthogonale directe dans $\mathbf{R}^4$;

— ou bien par une matrice 2×2 sur le corps $\mathbf{C}$ des complexes :

$$P = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \text{ avec } a = \delta + i\alpha,\ b = \beta + i\gamma$$

$$\text{et} \quad |a|^2 + |b|^2 = 1\,.$$

Le vecteur $\vec{v}$ de composantes (x,y,z) étant lui-même représenté par une matrice du même type $Q = \begin{pmatrix} ix & u \\ -\bar{u} & -ix \end{pmatrix}$ la matrice représentant $\rho(\vec{v})$ est alors $Q' = P\,Q\,P^*$, où P^* est la matrice adjointe de P (c'est-à-dire la transposée de la conjuguée) ; on remarque que P est alors une matrice unitaire dans $\mathbf{C}^2$ ($u = y + iz$).

Ce genre de représentations pose de délicats problèmes d'interprétation géométrique. Il en résulte qu'avec des lois de composition convenables, les ensembles de matrices de la forme M, ou H, ou P, avec les conditions imposées, constitueront des groupes *simples*, parce qu'isomorphes à $0^+(\mathbf{R}^3)$.

Remarque :

On pourrait imaginer assez facilement des méthodes d'exposition plus élémentaires ne faisant pas intervenir explicitement les classes de conjugaison ; mais ce genre de méthode, bien que fournissant en définitive une exposition plus brève et plus concise, offre l'inconvénient de masquer l'origine réelle des propriétés obtenues. La partition du groupe en classes de conjugaison est en effet la cause première de la plupart des propriétés des groupes, et en particulier par exemple des propriétés liées aux représentations,

soit comme groupes de substitutions, soit comme groupes d'endomorphismes d'un espace vectoriel. C'est ce qui a motivé de ma part le choix de ce système d'exposition, et qu'on ne m'en veuille pas de ne pas avoir adopté d'emblée un point de vue plus directement calculatoire.

LES PUBLICATIONS DE L'A.P.M.E.P.

L'A.P.M.E.P. a décidé, en 1960, de publier des livres ou des brochures écrits par un ou plusieurs de ses membres et pouvant servir au progrès de l'enseignement des mathématiques.

Les tirages des premiers titres de sa collection "*Les brochures de l'A.P.M.*" ayant été limités, ils ont été rapidement épuisés. Restent disponibles, parmi les derniers ouvrages parus :

Le Cours de l'A.P.M. — 3. *Eléments de topologie*, par A. et G. Revuz, 1966, 250 p., prix 27 F.

Bibliothèque d'Enseignement Mathématique, nouvelle collection d'ouvrages pour la formation permanente des maîtres :

1. *Pour apprendre à conjecturer : initiation au Calcul des Probabilités*, par MM. Guerber et Hennequin, 1968, 232 p., prix 25 F (cartonné 30 F).

2. *L'enseignement de la mécanique*, par P. Germain, R. Mazet, J. Kampé de Fériet, 1961 (40 p.) ; prix 2 F (3,15 F port compris).

3. *La mathématique parlée par ceux qui l'enseignent* par la Commission du Dictionnaire de l'A.P.M.E.P. Edition 1967 (A), prix 25 F. Millésime 1968 (B), prix 4 F. Edition 1968 (A, B), prix 27 F. Millésime 1969 (C), prix 5 F. Edition 1969 (A,B,C), prix 32 F. Millésime 1970 (D), prix 5 F. Edition 1970 (A,B,C,D), prix 37 F. Millésime 1971 (E), prix 5 F. Edition 1971 (A,B,C,D,E), prix 42 F. Millésime 1972 et 1973 (F), prix 5 F. Edition 1973 (A,B,C,D,E,F), prix 47 F. Millésime 1974 et 1975 (G), prix 5 F. Edition 1975 (A,B,C,D,E,F,G), prix 52 F.

Bibliothèque d'Information sur l'enseignement mathématique, brochures qui ne sont ni des manuels, ni encore moins des traités et qui devraient avoir le caractère incisif des libelles ...

1. *Charte de Chambéry*, 1969, 1971, 1973, 1976, 1980... étapes et perspectives d'une réforme de l'enseignement des mathématiques, octobre 1968, 32 p., prix 2 F.

2. *Matériaux pour l'histoire des nombres complexes*, par Jean Itard, Janvier 1969, 32 p. illustrées, prix 3 F.

4. *Angles*, par J. Frenkel, février 1971, 32 p., prix 3 F.

5. *Eléments de logique pour servir à l'enseignement mathématique*, par J. Adda et W. Faivre, février 1971, 52 p., prix 4 F.

6. *Charte de Caen*, prix 3 F.

7. *Musique classique et mathématique moderne*, par B. Parzysz, 32 p., prix 3,50 F.

8. *Mots* I, brochure 74, prix 6 F (8 F port compris). *Mots* II, brochure 75, prix 6 F (8 F port compris).

9. *Elem-Math* I, brochure 75, prix 3 F (4,15 F port compris).

10. *Carrés magiques*, Belouze, Glaymann, Haug et Herz, 48 pages, prix 4 F (5,15 Fport compris).

Conditions de vente et d'expédition

Les ouvrages précédents ne sont pas en vente en librairie. Pour se les procurer, opérer de la façon suivante :

1° Rédiger une formule de virement postal au compte de l'A.P.M.E.P. : Paris 5708-21, du montant des livres demandés (les prix sont compris franco de port).

2° Bien préciser *au dos du virement* les titres des ouvrages commandés.

3° Envoyer les trois volets du virement, sous enveloppe timbrée, au Secrétaire administratif de l'A.P.M.E.P. :

M. BLONDEL
154 avenue Marcel Cachin, 92320-Châtillon-sous-Bagneux.

Vous recevrez les ouvrages commandés en paquet-poste dans le plus court délai.

Note importante : Pour les brochures figurant sous les rubriques 8, 9, 10, vous pouvez vous adresser directement à votre Régionale (voir les adresses au début du Bulletin) qui en possède un stock à votre disposition (mêmes conditions de prix). Vous aiderez ainsi la trésorerie de votre Régionale qui perçoit une ristourne sur chaque brochure vendue.

Les ouvrages cités ci-dessus sont édités au prix coûtant. Aucune remise ne peut donc être consentie à quelque titre que ce soit. Aucun des ouvrages précédents n'est vendu en librairie.

Le secrétaire de l'A.P.M.E.P. participe également à la diffusion des oeuvres complètes d'Evariste Dupont dont le seul ouvrage paru est : *Apprentissage mathématique I*, un volume de 248 p., (Sudel éditeur) (Prix : 15 F franco pour les membres de l'A.P.M.E.P.).

Une ancienne brochure de l'A.P.M.E.P. :

L'ENSEIGNEMENT DE LA MECANIQUE

reste disponible : l'exemplaire 2 F (franco 3,50 F)

Au sommaire de cette brochure de 40 pages :

Paul GERMAIN : Principes et notions fondamentales de la mécanique classique.

R. MAZET : Les méthodes de la mécanique vibratoire des structures déformables.

J. KAMPE DE FERIET : Les équations fondamentales de la mécanique des milieux continus.

P. GERMAIN : Pour l'introduction d'éléments de dynamique dans le programme de Mathématiques de la classe de Mathématiques Elémentaires.

Publication A.P.M.E.P.

Prochainement un nouvel ouvrage de la bibliothèque de travail du professeur de mathématique :

A LA RECHERCHE DU NOYAU DES PROGRAMMES DU 1er CYCLE

(Savoir minimum en fin de troisième)

200 pages (*) (format Bulletin), 50 notices environ, par une Commission A.P.M.E.P. avec la participation d'I.R.E.M.S.

Ces notices regrouperont les termes mathématiques, notations, énoncés, "savoir-faire", méthodes et attitudes ... qui paraissent constituer le bagage minimum d'un élève sortant du premier cycle, après y avoir suivi une scolarité la plus proche possible des conditions normales.

Cette brochure est à l'usage du professeur. Elle se veut adaptée à un "*enseignement pour tous*".

Il ne paraît pas indispensable de rappeler qu'elle est le fruit d'un travail d'équipe.

Prix après parution : 15 F (port compris : 18 F)

Parution prévue pour courant Mai 1976.

Voir dans le Bulletin 300 :
page 581, une notice extraite de la future brochure ;
page 439, un article sur la brochure.

(*) ou davantage

Publications A.P.M.E.P.

Bibliothèque de travail du professeur de mathématique

Les CARRES MAGIQUES

Brochure de 48 pages sur un "thème vertical"

Pour vous la procurer, adressez-vous à votre Régionale APM

Prix : 4 F par la poste : 5,15 F

ASSOCIATION DES
PROFESSEURS DE MATHEMATIQUES
DE L'ENSEIGNEMENT PUBLIC

29, rue d'Ulm - 75005 Paris

Qu'est-ce que l'A.P.M.E.P. ?

L'Association des Professeurs de Mathématiques de l'Enseignement Public a été fondée en 1910. Réunissant à ses débuts des professeurs de l'enseignement secondaire public, elle a progressivement étendu son recrutement à tous les degrés de l'Enseignement public : premier degré, second degré classique et technique, supérieur. A la fin de 1975, elle réunit **quinze mille membres.**

Les maîtres qui enseignent des mathématiques à tous les niveaux, "**de la Maternelle à l'Université**", mettent en commun leurs expériences pédagogiques, se réunissent pour en discuter ou pour perfectionner leur culture scientifique. Ils ont défini leurs objectifs dans la Charte de Caen, en particulier sur les finalités de l'enseignement, l'expérimentation pédagogique, la formation des maîtres. En s'appuyant sur les idées contenues dans cette Charte, ils conjuguent leurs efforts pour améliorer l'enseignement des mathématiques (contenu, méthodes, etc...).

L'A.P.M.E.P. s'intéresse donc à toutes les questions qui concernent l'enseignement des mathématiques depuis les premières initiations (à la Maternelle et à l'Ecole Elémentaire) jusqu'aux études supérieures (recherche et formation des maîtres), sans oublier la formation permanente. En liaison avec les autres Associations de spécialistes et avec les organisations syndicales (en concurrence de qui elle ne se place jamais), elle s'attache à la sauvegarde des droits de la fonction enseignante et contribue à sa promotion.

L'A.P.M.E.P. entretient des relations amicales, échange des informations et des services, avec des Associations de Professeurs de Mathématiques des autres pays de l'Europe et du Monde.

L'Association est organisée en Régionales académiques (certaines avec des sections départementales) qui ont leurs activités pédagogiques propres. Une collaboration souvent fructueuse s'est instaurée avec les I.R.E.M. sur des objectifs communs.

Un Comité national élu par correspondance, renouvelé par quart chaque année, désigne un Bureau qui assure le fonctionnement administratif de l'Association, exécute les décisions de l'Assemblée générale et représente l'Association auprès des autorités de l'Education Nationale.

Chaque année, l'A.P.M.E.P. organise des journées d'étude sur des thèmes pédagogiques et scientifiques (moyens audiovisuels, mise en application de la Réforme à divers niveaux, mathématisation du réel, etc...).

L'A.P.M.E.P. édite un Bulletin (5 numéros par an) qui réunit des articles de documentation mathématique et pédagogique. Elle édite aussi des recueils de sujets d'examens ou concours : B.E.P.C., E.N., Baccalauréat, D.E.U.G.

Depuis 1960, l'A.P.M.E.P. édite des ouvrages de documentation pour les maîtres et les vend au prix coûtant. Devançant toute organisation administrative du "recyclage", elle a fourni aux maîtres soucieux de rénover leur enseignement une documentation abondante spécialement conçue pour eux, par des collègues particulièrement compétents et dévoués (consulter la liste des ouvrages dans le Bulletin). La diversité du contenu de ces brochures permet à chaque adhérent de choisir, quel que soit son niveau d'enseignement.

L'efficacité du travail de l'A.P.M.E.P. tient au nombre et au dynamisme de ses membres. Si vous ne les avez pas encore rejoints, faites-le donc sans tarder.

Liste des sections régionales et départementales

arrêtée au 1.11.75. Pour chaque section, nous donnons l'adresse d'un animateur à qui les Collègues s'adresseront pour avoir des informations supplémentaires sur l'activité de sa section. Entre crochets [ ], nous donnons les numéros des départements qui sont du ressort de la régionale. Entre doubles parenthèses (( )) le numéro de chèque postal quand il y a lieu (sauf avis contraire, l'intitulé du compte est "Régionale A.P.M.E.P. de...").

AIX-MARSEILLE [04, 05, 13, 84]
Pierre NOE, 49 rue Daumier, 13008-Marseille ((Marseille 28-94-82)).
AMIENS [02, 60, 80]
Jean CAPRON, 12 rue A. Chénier, Les Primevères, 80000-Amiens. Tél. (22) 92.16.79 ((Lille 862-04)).
Janine PROTIN, résidence de l'Abbaye, A36, rue du Dr Calmette, 60200-Compiègne.
BESANCON [25, 39, 70, 90]
Martial THIRIOT, I.U.T., 30 avenue de l'Observatoire, 25000-Besançon ((Dijon 2505-45 V)).
Section du Jura : ROBBE, Les Prés Cantaux, 39-Salins.
Section de Belfort : J. DAUTREVAUX, 41 rue du Château-Essert, 90000-Belfort.
BORDEAUX [24, 33, 40, 47, 64]
Pierre LOUQUET, 47 cours de la Somme, 33000-Bordeaux ((Bordeaux 3902-91)).
Section de la Dordogne : Mlle MARCHIVIE, 12 rue des Vaures, 24100-Bergerac.
Section de la Gironde : TEXTIER, Boutus, Beychac et Caillau, 33-Saint-Germain-du-Puch.
Section des Landes : LAVIGNE, 40-Aire-sur-Adour.
Section du Lot-et-Garonne : DE LATAULADE, 1 rue Claude Rivemale, 47-Villeneuve-sur-Lot.
Section des Pyrénées-Atlantiques : CELHAY, allée de la Forêt, 64600-Anglet.
BREST [29]
LE ROUX, 24 rue de Vendée, 29-Brest ((Rennes 25-5927)).
CAEN [14, 50, 61]
Jacky COCHEPIN, rue de la Chasse, 14290-Mathieu ((Rouen 1084-56 M)).
CLERMONT-FERRAND [03, 15, 43, 63] ((Clermont 1569-75))
André HENNETON, Sauvagnat Ste Marthe, 63500-Issoire.
DIJON [21, 58, 71, 89]
O. RENAUT, 38 bd. de l'Université, 21-Dijon ((Dijon 1751-05 V)).
Section de l'Yonne : D. REISZ, 11 rue du Saule, 89610-Vincelles.
Section de la Saône-et-Loire : MICHELOT, 32 avenue Boucicaut, 71100-Chalon-sur-Saône.
Section de la Nièvre : PUISSEGUR, 2 place de la Résistance, 58000-Nevers.
Section de Mâcon : Mlle DOMINIQUE, rue du Lavoir Charnay, 71000-Mâcon.
GRENOBLE [07, 26, 38, 73, 74]
C. BENZAKEN, 17 avenue du Vercors, 38240-Meylan ((Grenoble 349-49 U)).
Section de Chambéry : COMPAIN, Lycée Technique, 1 avenue du Colombier, 73000-Chambéry.
Section de Vienne : CHARNAY, Establin, 38780-Pont-Evêque.
Section d'Annecy : VIDIANI, B.P. 316, 74000-Annecy.
LILLE [59, 62]
MAS, Lycée Faidherbe, rue A. Carrel, 59-Lille ((Lille 4242-55)).
Section du Pas-de-Calais : LAURENT, 15 rue Albert-1er, 62-Arras.
LIMOGES [19, 23, 87]
UER des Sciences, 123 rue Albert Thomas, 87100-Limoges ((Limoges 117-66 P)).
Section d'Egletons : HAKENHOLZ, CES Albert Thomas, 19300-Egletons.
LYON [01, 42, 69]
Gilbert CROS, 86 avenue Jean-Jaurès, 69007-Lyon ((Lyon 7081-18)).
Section de Saint-Etienne : M. BOUTEILLE, Résidence de l'Hippodrome, Bât. D4, 42390-Villars.
Section de Bourg : R. CHARNAY, E.N., 01-Bourg-en-Bresse.
MONTPELLIER [11, 30, 34, 48, 66]
Mme FUCHS, 10 rue des Glaïeuls, 34-Montpellier ((Montpellier 385-25 W)).
Section du Gard : J. CHABRIER, 10 rue de Loye, 30000-Nîmes.
Section des Pyrénées Orientales : GALTIE, 16 rempart Villeneuve, 66-Perpignan.
Section de l'Aude : Mlle CABANEL, Lycée Lacroix, 11-Narbonne.
NANCY [54, 55, 57, 88]
MIRGAUX, 76 rue G. Mouilleron, 54-Nancy ((Nancy 1394-64 S)).
Section de la Moselle : E. SAUVADET, 17 rue du Fort, Longeville-les-Metz, 57000-Metz.
NANTES [44, 49, 53, 72, 85]
Mme PEYROT, 41 Les Hauts de l'Erdre, 44240-La Chapelle/Erdre.
Section de la Sarthe : KLAEYLE, 2 impasse Fizeau, 72100-Le Mans.
NICE [06, 20, 83] ((Marseille 5758-43))
J. MARIA, 5 ter rue Edith Cavell, 06000-Nice.
Section du Var : M.J. PAPAZIAN, La Colle d'Artaux, 83500-La Seyne.
ORLEANS-TOURS [18, 28, 36, 37, 41, 45]
P. MONSEILLER, Département de Mathématiques, Université d'Orléans, 45045-Orléans Cedex ((La Source 1440-09)).
Section de Tours : Monique GODICHEAU, Appt. 235, 14 rue Léonard de Vinci, 37170-Chambray-lès-Tours.
Section de Montargis : KISTER, 52 rue des Vignes, 45120-Chalette.
PARIS [75, 77, 78, 91, 92, 93, 94, 95]
J. ADDA, 10 rue Vandrezanne, 75013-Paris.
Section de la Seine-Saint-Denis : M. LOI, 68 rue des Ecoles, Bât. A 318, 93300-Aubervilliers.
((Régionale Parisienne de l'A.P.M.E.P. Paris 25 108 63)).
Bulletin de la Régionale : Gilbert GRIBONVAL, 129 avenue du Général Leclerc, 91120-Palaiseau.
POITIERS [16, 17, 79, 86]
J. BOROWCZYK, 1 rue de Provence, 86000-Poitiers ((Bordeaux 38-52-59)).
Section des Deux Sèvres : FROMENTIN, 29 avenue de Nantes, 79000-Niort.
Section de la Charente : MARRON, CES La Grande Garenne, rue Pierre Aumaître, 16000-Angoulême.
Section de la Charente Maritime : Y. DARDANT, 25 rue Philippe Vincent, 17000-La Rochelle.
REIMS [08, 10, 51, 52]
THIERUS, 57 rue David, 51100-Reims ((Châlons-sur-Marne 1262-80 L)).
Section des Ardennes : ZILLI, 8 Le Grenet Riglemont, 08100-Charleville Mézières.
Section de l'Aube : HAUBRY, 16 A rue Jules Didier, 10120-Saint-André-les-Vergers.
Section de la Haute-Marne : Mlle GODON, 8 rue de Lorraine, 52000-Chaumont.
Section de la Marne : SCHACHERER, 26 rue du Moulin à Vent, 51200-Epernay.
RENNES [22, 35, 56]
LEVEILLEY, 28 avenue des Vignes, Châtillon-sur-Seiche, 35230-St-Erblon ((Rennes 1707-29)).
ROUEN [27, 76]
Michèle CHOUCHAN, 16 rue du Bailliage, 76000-Rouen ((Rouen 1350-13 D)).
Section du Havre : PESTEL, 2 rue J. Langlois, 76-Le Havre.
STRASBOURG [67, 68]
SYLVESTRE, 17 rue Grimling, 67200-Strasbourg.
Section du Haut-Rhin : LEVASSORT, 27 rue Georges Sand, 68-Mulhouse-Dornach.
Section de l'Allemagne Fédérale : G. TOUYET, S.P. 69.037 F.F.A.
TOULOUSE [09, 12, 31, 32, 46, 65, 81, 82]
Line MAILHOS, Université Paul Sabatier, 31077-Toulouse Cedex ((Toulouse 2035-51)).
Section de l'Ariège : Mme GALY, 96 avenue V. Pilhes, 09400-Tarascon-sur-Ariège.
Section de l'Aveyron : SCHIOPETTO, CES La Penderie, 12000-Rodez.
Section du Gers : Mlle BORIES, 29 rue de Metz, 32000-Auch.
Section des Hautes-Pyrénées : TARBOULIER, 36 rue M. Lamarque, 65000-Tarbes.
Section du Tarn-et-Garonne : FOURNIE, CES Bourdelle, boulevard Herriot, 82000-Montauban.
Section du Lot : Mme PICARD, E.N., av. Henri Martin, 46000-Cahors.
Section du Tarn : Christine MANDIRAC, Lycée de Carmaux, 81400-Carmaux.

Pour les nouveaux adhérents et les adhérents ayant changé de résidence :

COUPON DE MISE A JOUR DU FICHIER REGIONAL

A détacher et à envoyer d'urgence au Président de votre Régionale (adresse ci-dessus)

Nom : .....

Prénom : .....

Adresse personnelle : .....

Etablissement : .....

Fonction : .....

☐ **Nouvel adhérent**

☐ **Ancien adhérent muté dans la circonscription de la Régionale**

n° .....

Mettre une X dans la case convenable.

CONDITIONS D'ADHESION ET D'ABONNEMENT

(taux pour l'année 1976)

Abonnement (valable pour l'année civile) **80 F**

Pour les membres de l'A.P.M.E.P.

— **Cotisation d'adhésion : trois catégories**

A)	Instituteurs Retraités	**10 F**
B)	Membres dont l'indice de traitement est inférieur ou égal à 350	**20 F**
C)	Membres dont l'indice de traitement est supérieur à 350	**30 F**

— **Abonnement au Bulletin** **35 F**

Les adhérents sous les drapeaux bénéficient d'un abonnement gratuit d'un an.
La cotisation seule ne donne pas droit au service du Bulletin.
Les cotisations et/ou abonnements sont perçus par année civile ; cependant, en début d'année scolaire , les nouveaux adhérents peuvent opter pour une des deux solutions suivantes :

— adhérer et s'abonner, avec effet rétroactif : ils recevront les numéros parus pendant l'année civile en cours ; ils devront ensuite, comme les anciens adhérents, faire un versement pour l'année civile suivante, après réception d'une lettre d'appel de cotisation et d'abonnement ;
— adhérer et s'abonner pour l'année civile suivante : dans ce cas, il leur est adressé le dernier numéro à paraître dans l'année civile en cours.

L'abonnement au service du Bulletin donne droit à un service au choix parmi les rubriques suivantes :

— deux catégories de math-annales à choisir parmi quatre

ou

— une brochure : pour 1976, l'APMEP propose un choix parmi les cinq brochures suivantes :
Mots I ; Mots II ; Mots III ; Elem-Math I ; Elem-Math II .

Ce choix est fixé par une fiche jointe à l'appel de cotisation.

MODES DE PAIEMENT

1° Détacher et remplir complètement et très lisiblement la fiche d'adhésion ou d'abonnement au verso.

2° Remplir les trois volets d'un virement postal adressé à l'A.P.M.E.P., 29, rue d'Ulm, 75005 Paris. C.C.P. Paris 5 708-21.

3° Sous enveloppe affranchie adresser le tout, fiche rose et les trois volets du virement postal, au siège de l'A.P.M.E.P.

Note du Secrétariat : utilisez de préférence un chèque de virement à notre C.C.P. ou, à la rigueur, un chèque bancaire. Nous renverrons à son expéditeur tout autre mode de paiement.

4° Envoyer à votre régionale le coupon de mise à jour du fichier régional.

ATTENTION ! La présente fiche dite "fiche rose" est à utiliser EXCLUSIVEMENT POUR SOUSCRIRE UNE ADHESION (OU UN ABONNEMENT) A L'A.P.M.E.P.

Le RENOUVELLEMENT vous est automatiquement demandé par un "appel à coupon détachable" que vous recevrez courant Janvier.

POUR UN CHANGEMENT D'ADRESSE (OU D'ETAT CIVIL) : porter sur une feuille, **et non au dos d'un chèque**, l'ancienne adresse (ou l'ancien état civil), *rappeler le numéro de votre carte A.P.M.E.P.*, puis donner les renseignements nouveaux ; envoyer cette feuille sous enveloppe timbrée au siège de l'A.P.M.E.P.

Note du Secrétariat : impossible de retrouver rapidement et sans erreur votre fiche si vous n'indiquez pas votre numéro A.P.M. (lequel est rappelé sur la bande ou l'étiquette-adresse du Bulletin).

SI VOUS ENSEIGNEZ MATHEMATIQUES ET BIOLOGIE, vous pouvez, pour une cotisation de 30 F et un abonnement jumelé réduit de 40 F, participer aux activités des deux associations APBG et APMEP.
Demandez pour cela au siège, 29, rue d'Ulm, 75005 Paris, une fiche d'adhésion "Maîtres polyvalents" (dite "fiche jaune").

Association des Professeurs de Mathématiques de l'Enseignement Public

A. P. M. E. P.

FICHE D'ADHESION OU D'ABONNEMENT

à remplir complètement et à adresser à l'A.P.M.E.P., 29, rue d'Ulm, 75005 Paris
accompagné des 3 volets d'un virement postal à A.P.M.E.P. Paris 5.708-21

M. - Mme - Mlle (Rayer les mentions inutiles)

Nom et prénom : _____
(en capitales d'imprimerie)

Adresse à laquelle vous désirez recevoir le Bulletin :

N° et rue : _____

(suite) _____

Code postal _____ Ville ou pays _____

Année de naissance : _____

NE RIEN ECRIRE DANS CE CADRE

Nom et adresse de l'établissement dans lequel vous enseignez : _____ (2)

Nom : _____

Adresse : _____

Département (en code) : _____ Ville : _____

Titres universitaires (1)

Bachelier ou équiv.	1	☐
C.A.P. - C.E.G.	2	☐
Licencié	3	☐
Certifié	4	☐
Agrégé	5	☐
Docteur	6	☐
Autres (maîtrise, etc.)	7	☐

La plus grande partie de votre service est effectuée dans (1) :

Ens. pré-élémentaire	1	☐	Cl. préparatoires	7	☐
Ens. élémentaire	2	☐	Ecole normale	8	☐
C.E.G. - C.E.T.	3	☐	I.U.T.	9	☐
C.E.S.	4	☐	Ens. sup. 1er cycle	10	☐
Lycée 1er cycle	5	☐	Ens. sup. 2e, 3e cycle	11	☐
2e cycle	6	☐	Administration	12	☐
			Inspection	13	☐

Nouvel adhérent ☐
Ancien adhérent ☐

Année de la première adhésion _____

Versement pour l'année civile 197☐ Indice de traitement _____

Cotisation d'adhésion à l'APMEP (consulter la page 3)

Adhérents	Catégorie A	10 F	☐*
	Catégorie B	20 F	☐
	Catégorie C	30 F	☐

Bulletin - Abonnement annuel

Etablissements - Bibliothèques - Non adhérents	80 F	☐*
Adhérents APMEP	35 F	☐

Attention ! La cotisation seule ne donne pas droit au service du Bulletin.

Je joins le titre de paiement complet correspondant à la catégorie choisie : 80 - 65 - 55 - 45 - 30 - 20 - 10 F et j'adresse le tout sous enveloppe timbrée à l'APMEP, 29 rue d'Ulm, 75005 Paris.

A ....., le .....
Signature

(1)* Mettre une croix dans la case qui convient
(2) Ne rien inscrire dans ces cases