PRINCIPES DE COMBINATOIRE

PAR

C. BERGE
Directeur de Recherches au C. N. R. S.
Chargé de cours à la Faculté des Sciences de Paris

DUNOD
PARIS
1968

Table des matières

CHAPITRE 3

FORMULES D'INVERSION ET APPLICATIONS

CHAPITRE 4

GROUPES DE PERMUTATIONS

CHAPITRE 5

LA MÉTHODE DE POLYA

Qu'est-ce que la Combinatoire ?

On parle beaucoup de nos jours de la Combinatoire (ou la « Combinatorique ») ; et pourtant ni les encyclopédies ni les ouvrages d'initiation ne semblent donner une définition satisfaisante de cette science aux ramifications multiples.

En fait, le mathématicien sent d'instinct que certains problèmes sont de « nature combinatoire », et que les méthodes pour les résoudre méritent d'être étudiées systématiquement. C'est en tout cas ce que dit POLYA en préfaçant le premier volume du nouveau *Journal of Combinatorial Theory* (1).

La définition de la Combinatoire que nous voulons proposer ici, repose sur la notion bien précise de « configuration ».

On cherche une *configuration* chaque fois que l'on veut placer des objets de façon à respecter certaines contraintes fixées à l'avance. Le rangement de paquets de tailles diverses dans un tiroir trop petit est une configuration.

Prenons un exemple de bi-carrés latins orthogonaux d'ordre 10, soit :

---

(1) Academic Press, New York et Londres. Ce journal a débuté en 1966.

Aa	Gh	Fi	Ej	Jb	Id	Hf	Bc	Ce	Dg
Hg	Bb	Ah	Gi	Fj	Jc	Ie	Cd	Df	Ea
If	Ha	Cc	Bh	Ai	Gj	Jd	De	Eg	Fb
Je	Ig	Hb	Dd	Ch	Bi	Aj	Ef	Fd	Gc
Bj	Jf	Ia	Ac	Ee	Dh	Ci	Fg	Gb	Ad
Di	Cj	Jg	Ib	Hd	Ff	Eh	Ga	Ac	Be
Fh	Ei	Dj	Ja	Ic	He	Gg	Ab	Bd	Cf
Cb	Dc	Ed	Fe	Gf	Ag	Ba	Hh	Ii	Jj
Ec	Fd	Ge	Af	Bg	Ca	Db	Ij	Jh	Hi
Gd	Ae	Bf	Cg	Da	Eb	Fc	Ji	Hj	Ih

Ici, les objets sont les éléments du produit cartésien

$$\{A, B, C, D, E, F, G, H, I, J\} \times \{a, b, c, d, e, f, g, h, i, j\}$$

que l'on applique dans les 100 cases du carré de 10×10. Les contraintes sont :

1) l'application est bijective : un couple dans chaque case et tout couple figure une fois et une fois seulement dans le tableau ;

2) il n'y a pas deux fois la même lettre majuscule (ni minuscule) dans la même ligne, ni dans la même colonne.

C'est là une des configurations les plus remarquables de l'histoire de la Combinatoire depuis EULER, qui conjecturait qu'elle ne pouvait exister. La conjecture d'EULER fut démentie seulement en 1960 par BOSE, PARKER et SHRIKHANDE, qui ont montré en outre l'existence d'un tel tableau pour tout ordre différent de 6.

On pourrait mathématiser le concept de configuration en le définissant comme une *application d'un ensemble d'objets dans un ensemble abstrait fini muni d'une structure connue* ; par exemple une permutation de n objets est une « application bijective de l'ensemble des objets dans l'ensemble ordonné 1, 2, ..., n ». Néanmoins, on ne s'intéresse qu'aux applications *qui satisfont à certaines contraintes*, et la nature de ces contraintes est trop variée pour requérir à un tel degré de généralité.

De même que l'Arithmétique étudie les nombres entiers (avec les opérations classiques), que l'Algèbre étudie les opérations en général, que l'Analyse étudie les fonctions, que la Géométrie étudie les formes rigides et la Topologie celles qui ne le sont pas, la Combinatoire étudie, elle, les configurations. Elle veut

démontrer l'existence de configurations d'un type voulu, ou les dénombrer, ou les recenser ; elle cherche leurs propriétés intrinsèques ; elle étudie les transformations d'une configuration en une autre, aussi bien que les « sous-configurations » qu'on peut extraire d'une configuration donnée.

Ces préoccupations sont exactement les mêmes que celles des autres branches des mathématiques modernes. Néanmoins, il est surprenant de constater que la Combinatoire s'est développée en marge ou à l'ombre des grands courants. Les théorèmes élémentaires ont été oubliés et redécouverts plusieurs fois. Le mathématicien polycéphale Nicolas BOURBAKI ne mentionne guère le théorème de POLYA ; dans ses quelque vingt volumes déjà parus, on ne relève d'ailleurs aucun théorème combinatoire général, quoique certaines formules indispensables soient distillées dans le texte au fur et à mesure des besoins. Il est urgent d'éviter un tel malentendu.

Premier aspect : l'étude d'une configuration connue

La première phase dans le développement des mathématiques combinatoires a consisté à étudier les propriétés intrinsèques d'une configuration connue, ou dont la construction ne présente guère de difficultés. Dès le début de notre ère, le système divinatoire connu sous le nom de Géomancie (1) s'est occupé d'analyser des configurations aléatoires. Dans une lettre adressée par ARCHIMÈDE à ERATHOSTÈNE, il est proposé de calculer le nombre de bêtes à corne du Dieu Soleil : « Lorsque la foule des taureaux blancs se mêlait à celle des taureaux noirs, ils formaient un carré dont la surface était celle de la Sicile ; et les taureaux roux réunis aux taureaux tachetés formaient une figure triangulaire ayant un animal au sommet et chaque rang croissait successivement d'une unité jusqu'au dernier rang, sans qu'il manquât ou restât l'une de ces bêtes » (2).

Ce problème, une des rares allusions de l'antiquité aux mathématiques combinatoires, relève en fait principalement de l'arithmétique, ainsi d'ailleurs que les nombres polygonaux de PYTHAGORE, NICOMACHE, DIOPHANTE. Il a fallu attendre EULER pour retrouver chez les mathématiciens de la Combinatoire véritable.

---

(1) Cf. R. JAULIN, *La Géomancie, Cahiers de l'Homme*, Mouton éd., Paris-La Haye 1966.

(2) Cité par CALLANDREAU, « Célèbres problèmes mathématiques », et par LESSING en 1773. Il est remarquable de noter que ce problème aboutit à l'équation de FERMAT :

$$y^2 - 410.286.423.278.424\, x^2 = 1 .$$

La plus petite solution pour l'effectif du troupeau serait de l'ordre de $7.766\ 10^{206.541}$.

Deuxième aspect : la recherche d'une configuration inconnue

Un autre aspect de la Combinatoire consiste à démontrer l'existence ou la non-existence d'une configuration ayant certaines propriétés remarquables. C'est le cas du problème célèbre des 9 ponts de la ville de Königsberg (aujourd'hui Kaliningrad) ; ou celui des 36 officiers d'EULER ; ou d'une façon plus abstraite de la construction de géométries finies. Il est assez troublant de constater que ce type de recherche existe dans le Yi-King (1), le livre divinatoire utilisé en Chine par les moines taoïstes, et aussi l'un des plus vieux textes

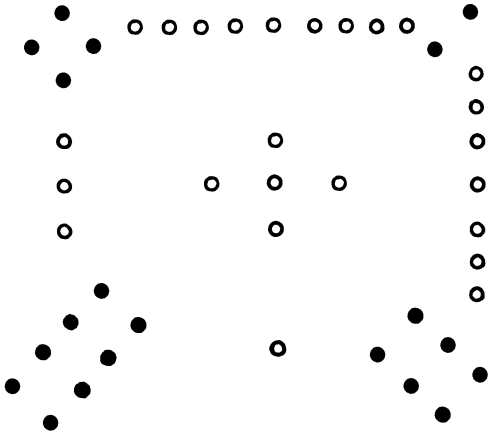


FIG. 1. — Le Grand Plan.

humains existant actuellement (environ 2200 avant J.-C.). Cet ouvrage sacré décrit en effet deux configurations, le « Grand Plan » (Lo-chou) et le « Tableau du Fleuve » (Ho-t'ou). Le « Grand Plan », qui d'après la légende, émergea de la rivière Lo porté par une tortue, est donné sur la figure 1 ; si on le transcrit en chiffres européens, il donne un carré magique célèbre dit de « Saturne » :

4	9	2
3	5	7
8	1	6

(1) Cf. « Le Yi-King, ou livre des changements de la dynastie des Tscheou », traduit pour la première fois en français par L. F. PHILASTRE, *Annales du Musée Guimet*, Paris, Leroux 1885-1893, vol. 2, p. 511.

Cf. aussi : « The Yi-King », traduit en anglais par J. LEGGE (Oxford Clarendon Press, 1882). La liste des travaux européens sur le Yi-King est donnée par H. WUTTKE, *Die Entstehung der Schrift*, Leipzig 1875 ; et par M. GRANET, *La Pensée Chinoise*, Paris.

Configuration de nombres extrêmement remarquable, la somme des éléments d'une rangée, ou d'une colonne, ou d'une diagonale, étant toujours égale à 15.

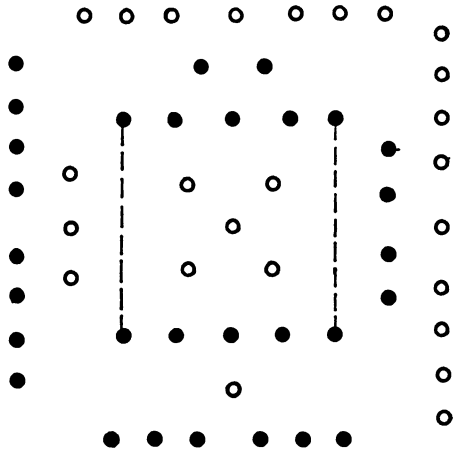


FIG. 2. — Le Tableau du Fleuve.

Le « Tableau du Fleuve », qui fut également d'après la légende porté par une tortue sacrée, est reproduit par la figure 2 ; transcrit en chiffres arabes. il donne la configuration suivante :

				7				
				2				
			10		10			
8		3		5		4		9
			10		10			
				1				
				6				

On peut voir que la somme de deux chiffres adjacents de ce tableau se retrouve en additionnant les chiffres qui occupent les positions homométiques par rapport au centre : $5 + 3 = 8$, $5 + 1 = 6$, etc. $3 + 10 + 2 = 8 + 7$; $3 + 10 + 1 = 8 + 6$, etc.

Si l'on connaît la difficulté qu'il y a à construire de telles configurations, on ne peut manquer de constater que la Combinatoire existait dans l'antiquité chinoise.

Troisième aspect : le dénombrement exact des configurations

Pour certaines configurations spécifiques que l'on obtient sans peine, comme les combinaisons de n objets pris p à p, il est naturel de se demander combien il y en a ; une nouvelle étape dans l'évolution de la Combinatoire consistera donc à exprimer par une formule le nombre de configurations ayant des propriétés données.

Bien entendu, c'est sous la poussée magistrale du Calcul des Probabilités et de la Statistique que la Combinatoire s'est développée dans cette direction (de par la définition même de la « probabilité ») ; et pendant longtemps, la majorité des mathématiciens ont identifié « analyse combinatoire » et « dénombrement ». Pour J. RIORDAN ([1]), le but de la Combinatoire est de « trouver le nombre de façons d'opérer pour effectuer certaines opérations bien définies ».

Si l'on se borne à cet aspect, on constate un peu partout des débuts avortés de Combinatoire, la plupart des formules ayant été redécouvertes plusieurs fois à des occasions diverses. Par exemple, et en premier lieu, les coefficients binomiaux apparaissent au XII^e siècle chez l'arithméticien indien BHASKARA ; ils resteront néanmoins ignorés des occidentaux, jusqu'à PASCAL et FERMAT, qui les redécouvrent à l'occasion des jeux de hasard. Récemment, on s'aperçut que la méthode de récurrence pour obtenir ces coefficients binomiaux et le « triangle de Pascal » étaient enseignés en 1265 par un philosophe persan, NASIR-AD-DIN ([2]). On sait aussi que vers 1560, CARDAN indique que le nombre de parties d'un ensemble à n éléments est 2^n.

En 1666, LEIBNIZ, à l'âge de 20 ans à peine, publiait le premier traité de Combinatoire : « Dissertatio de Arte Combinatoria ». Il expliquait dans sa préface comment il entrevoyait une discipline nouvelle, ayant des ramifications en logique, histoire, et même en morale, en métaphysique et « à l'univers des Sciences » !

Au fur et à mesure que les configurations à dénombrer devenaient plus complexes, et principalement avec Euler, l'Analyse Combinatoire s'est intéressée aux outils ; la plupart des probabilistes, statisticiens, ingénieurs qui se sont intéressés à compter, ont aussi indiqué leurs recettes. Les deux découvertes les plus célèbres de cet ordre d'idées sont les fonctions génératrices découvertes par LAPLACE mais déjà utilisées auparavant implicitement par EULER ; et le théorème attribué à G. POLYÀ, mais qui semble avoir été auparavant connu de

---

([1]) J. RIORDAN, *An Introduction the Combinatorial Analysis*, Wiley, New York 1958.

([2]) NASIR-AD-DIN AT-TUSI, *Petit Livre d'arithmétique par tableaux et tables*. Traduction russe par S. A. AHMEDOV et B. A. ROSENFELD, *Istor. Mat. Issled*, **15**, 1963, 431-344 (*Math. Rev.*, **31**, 1966, p. 1040).

REDFIELD [1]. C'est du moins ce que clame BLANCHE DESCARTES, dans un poème que nous nous devons de citer :

« ENUMERATIONAL. »
Polyà had a theorem
(Which Redfield proved of old).
What secrets sought by graphmen
Whereby that theorem told !

So Polyà counted finite trees
(As Redfield did before).
« Their number is exactly such,
And not a seedling more. »

Harary counted finite graphs
(Like Redfield, long ago),
And pointed out how very much
To Polyà's work we owe.

And Read piled graph on graph on graph
(Which is what Redfield did).
So numbering the graphic world
That nothing could be hid.

Then hail, Harary, Polyà, Read,
Who taught us graphic lore,
And spare a thought for Redfield too,
Who went too long before.

(Blanche Descartes).

Quatrième aspect : le Dénombrement approximatif des Configurations

Lorsqu'il s'agissait seulement de « compter », la Combinatoire était une collection de recettes éparses, et cet aspect essentiellement artisanal a produit de nombreuses formules arithmétiques, fort belles et souvent surprenantes. Pour cette raison, la Combinatoire a été pendant deux siècles annexée à la Théorie des Nombres.

Au XX^e siècle, de nouvelles applications sont apparues : En chimie (il ne faut pas oublier que c'est pour dénombrer des polymères que Polyà énonça

---

(1) J. H. REDFIELD, The Theory of Group-reduced Distributions, *Am. J. Math.*, **49**, 1927, pp. 433-455.

son fameux théorème) ; en physique (le problème des dimères) ; en Economie et en Recherche Opérationnelle (le problème du voyageur de commerce) ; en Statistique (les plans d'expérience) ; en Théorie de l'Information (problème de la capacité d'un ensemble de signaux), etc.

Lorsque les configurations à étudier devenaient trop capricieuses, il s'avérait inutile de tenter de les rattacher à des structures algébriques connues, et à les dénombrer par de « belles formules » : à défaut d'égalités, on a dû recourir à des inégalités, à des comportements asymptotiques, à des congruences modulo p, etc.

Au lieu de chercher le nombre des configurations avec une propriété donnée, on cherche certaines informations sur ce nombre sans donner de formules exactes ni même récurrentes. Un cas particulièrement curieux dans cet ordre d'idées est celui des nombres de RAMSEY, si proches des coefficients binomiaux, mais si insaisissables qu'on ne sait même pas les calculer lorsque les paramètres ont des valeurs supérieures à 7.

Cinquième aspect : l'énumération des Configurations

Si l'on s'intéresse aux nombres de configurations vérifiant certaines propriétés données, c'est un problème de *dénombrement* ; si l'on veut la liste de ces configurations, c'est un problème d'*énumération* (ou : *recensement*). (Il faut d'ailleurs noter que dans la langue anglaise le mot « enumeration » a le sens de « dénombrement ».)

Enumérer des configurations est une tâche souvent ingrate, parfois impossible à réaliser pour un être humain, et même pour un ordinateur à grande vitesse ; néanmoins, c'est encore le seul instrument de démonstration dans certains problèmes combinatoires particulièrement difficiles (raisonnements exhaustifs).

Des résultats importants de la Topologie ont été découverts à partir des listes de polyèdres convexes.

Le problème de l'énumération est inséparable du problème du classement : si l'on divise l'ensemble des configurations à étudier en classes, il suffit parfois de démontrer le résultat espéré sur un seul représentant de chaque classe.

Pour les cas très simples (par exemple : les combinaisons de n objets pris p à p), c'est en déterminant une méthode d'énumération que l'on obtient une formule de dénombrement ; mais l'inverse peut également se produire : les opérations arithmétiques (sur des nombres) peuvent se généraliser à des opérations algébriques (sur des ensembles de configuration), et une méthode de dénombrement devient un procédé pour engendrer des configurations. C'est ce qui s'est produit quand on a voulu recenser les chemins de longueur donnée dans un graphe [1] ;

---

[1] Cf. A. KAUFMANN et Y. MALGRANGE, Recherche des Chemins et Circuits hamiltoniens d'un graphe, *Revue Française de R. O.*, **26**, 1963. Voir aussi : A. KAUFMANN, *Initiation à la Combinatorique*, Dunod, Paris 1968.

il est vraisemblable que l'analyse combinatoire classique pourrait être réécrite dans cette optique.

Sixième aspect : l'optimisation

Depuis longtemps en Recherche Opérationnelle, on rencontre des problèmes du type suivant :

Ayant associé à toute configuration x avec des propriétés données une valeur numérique $f(x)$ (la fonction économique), choisir une configuration x_0 qui minimise $f(x)$; ou qui la rende ε-minimale, c'est-à-dire telle que

$$f(x) \geqslant f(x_0) - \varepsilon$$

pour toute configuration x avec les propriétés données.

C'est le cas du célèbre « problème du voyageur de commerce » : trouver l'itinéraire le plus court que doit choisir un voyageur de commerce s'il veut visiter une fois et une fois seulement toutes les capitales des 50 états des U. S. A. et revenir à son point de départ. Ce problème, d'apparence anodine, n'a guère jusqu'à ce jour trouvé de solution satisfaisante, les algorithmes proposés pour trouver l'itinéraire optimal comportant un nombre d'étapes trop élevé (pour un « bon » algorithme avec n points, l'ordre de grandeur du nombre d'étapes doit être un polynôme en n ; au-delà, on arrive très vite à ne plus pouvoir opérer, même avec un ordinateur).

Dans des cas particulièrement délicats, on a recours à des procédures approchées, du type « SEP » (1) ou du type « Branch and Bound » (méthode de LITTLE, MURTY, SWEENEY et KAREL (2) pour le problème du voyageur de commerce ; méthode de LAND et DOIG (3) pour la résolution des programmes linéaires mixtes, etc.).

Ces procédures consistent, grosso modo, à considérer de proche en proche des sous-ensembles de solutions acceptables, de plus en plus petits, jusqu'à pouvoir mettre en évidence une solution ε-optimale dans l'un d'eux (pour un ε que l'on estime suffisamment petit).

A côté de ce type de problèmes d'optimisation (que l'on pourrait appeler la « maximisation »), il en existe d'autres, qui consistent à choisir un ensemble de configurations acceptables selon des critères bien définis ; c'est le cas des problèmes de choix en présence de points de vue multiples (par exemple : la méthode ELECTRE (4)), de la recherche d'une « solution » d'un jeu non co-

(1) Voir principalement : P BERTIER et B. ROY. Une procédure de résolution pour une classe de problèmes pouvant avoir un caractère combinatoire, *ICC-Bulletin*, **4**, 1965.

(2) J. D. C. LITTLE, K. G. MURTY, D. W. SWEENEY et C. KAREL, An Algorithm for the Travelling Salesman Problem, *Operations Research*, **11**, 1963.

(3) A. G. DOIG et A. H. LAND, An Automatic Method for Solving Discrete Programming Problems, *Econometrica*, **28**, 1960.

(4) P. BUFFET, J. P. GREMY, M. MARC, B. SUSSMANN, Peut-on choisir en tenant compte de critères multiples, *METRA*, **VI**, 1967.

opératif à n joueurs (au sens de VON NEUMANN-MORGENSTERN), du « noyau » d'un graphe. En général, dans les cas mentionnés, il ne s'agit pas de choisir une configuration optimale, mais un ensemble de configurations qui méritent d'être retenues pour un choix ultérieur.

* * *

Si l'on regarde tous les aspects de la Combinatoire que nous avons essayé d'énumérer ici, on est frappé par la prolifération récente des problèmes qui peuvent se poser à propos de configurations, et de la diversité des outils pour les résoudre.

Un grand nombre de problèmes combinatoires peuvent être étudiés dans le cadre d'une théorie mathématique cohérente et bien constituée (Théorie des Graphes, Corps de Galois, Algèbres booléennes) ; mais il en existe d'autres, et la tâche la plus pressante sera de relier les méthodes existantes entre elles, de les formaliser, de les généraliser.

Le présent ouvrage s'occupe seulement des problèmes de dénombrement, c'est-à-dire une des préoccupations les plus anciennes de la Combinatoire ; c'est le texte d'un cours professé à la Faculté des Sciences de Paris en 1967-1968 dans le cadre de la Maîtrise de Mathématiques et Applications fondamentales.

Nous avons cru devoir rédiger ce cours dans l'optique de la Théorie des Ensembles, et ne pas utiliser l'ancienne terminologie (genre : « Combinaisons avec répétitions », etc.) devenue ambiguë.

En outre, aux applications classiques tirées de la théorie des fonctions spéciales ou de la théorie des nombres, nous avons préféré systématiquement des applications d'intérêt plus général ou provenant de domaines nouveaux comme la théorie de l'information.

Enfin, nous avons évité systématiquement l'emploi des calculs symboliques, qui sont parfois des outils commodes pour manipuler des formules trop compliquées, mais qui sont en général utilisés sans justification suffisante. On admet qu'une propriété qui se traduit par une égalité $|A| = |B|$ est mieux explicitée lorsque l'on construit une bijection entre deux ensembles A et B, plutôt qu'en calculant les coefficients d'un polynôme dont les variables n'ont pas de significations particulières [1].

---

[1] La méthode des fonctions génératrices, qui a exercé ses ravages pendant un siècle, est tombée en désuétude pour cette raison ; en tout cas, il ne saurait être question de l'exposer en dehors du cadre des anneaux de séries formelles (exposé par exemple dans : P. DUBREIL et M. L. DUBREIL-JACOTIN, *Leçons d'algèbre moderne*, Dunod éditeur, pp. 122-135).

1

Les fonctions élémentaires de dénombrement

§ 1. *Applications d'ensembles finis*

Un *ensemble fini* A est défini par une collection d'objets distincts $a_1, a_2, \ldots, a_m$. Les notations classiques sont :

$a \in A$,	a est un élément de l'ensemble A,
$\mid A \mid$,	cardinalité de A (nombre d'éléments de l'ensemble A),
$A \subset B$,	A est un sous-ensemble de B (tout élément de A est élément de B),
$A \cup B$,	réunion des ensembles A et B (ensemble des éléments qui appartiennent à A ou à B),
$A \cap B$,	intersection des ensembles A et B (ensemble des éléments qui appartiennent à la fois à A et à B),
$\bar{A} = X - A$,	complémentaire de A (ensemble des éléments qui appartiennent à X et non à A),
$\varnothing$,	ensemble vide (sans éléments),
$\mathcal{P}(A)$,	famille des sous-ensembles de A,
$A \times B$,	produit cartésien des ensembles A et B, (ensemble des couples (a, b) tels que $a \in A$, $b \in B$,
$A^n = A \times A \times \cdots \times A$,	ensemble des n-uples $a_1, a_2, \ldots, a_n$ pris dans A.

Considérons deux ensembles A et X ; les éléments de A sont désignés par $a_1, a_2, \ldots, a_m$; ceux de X par $1, 2, \ldots, n$. Une *application* de X dans A est une loi, notée

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_{i_1} & a_{i_2} & \ldots & a_{i_n} \end{pmatrix},$$

qui fait correspondre à l'objet 1 de l'ensemble X l'objet $a_{i_1} = \varphi(1)$ de l'ensemble A, à l'objet 2 l'objet $a_{i_2} = \varphi(2)$, etc.

PREMIÈRE INTERPRÉTATION : rangement de n objets.

Parfois, on assimile

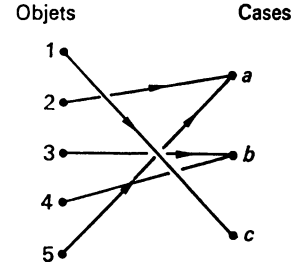
X à un ensemble d'objets à ranger,

A à un ensemble de cases où l'on range.

Une application de X dans A est alors une *façon de ranger* dans les cases.

Exemple. L'application.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & a & b & b & a \end{pmatrix}$$



représente le rangement :

des objets 2 et 5 dans la case a,
des objets 3, 4 dans la case b,
de l'objet 1 dans la case c.

DEUXIÈME INTERPRÉTATION : n-uple de symboles, ou « mot » de longueur n.

X est un ensemble de places numérotées 1, 2, ..., n,

A est un ensemble de symboles pour remplir les cases numérotées.

Une application de X dans A est alors un n-uple de symboles, certains symboles pouvant se répéter plusieurs fois.

Exemple. L'application

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & a & b & b & a \end{pmatrix}$$

représente le mot *cabba*, et l'on écrit parfois

$$\varphi = cabba\,.$$

Il y a ainsi une *dualité* entre les rangements de n objets et les mots de n lettres, qui sera souvent utilisée par la suite.

On dit qu'une application φ est *surjective* (ou une *surjection*) si pour tout élément $a \in A$, il existe au moins un $i \in X$ tel que $a = \varphi(i)$.

(Le rangement est alors avec au moins un objet dans chaque case ; le mot contient alors tous les symboles).

On dit qu'une application est *injective* (ou une *injection*) si

$$i \neq j \text{ entraîne } \varphi(i) \neq \varphi(j)$$

(le rangement est alors avec pas plus d'un objet dans chaque case ; le mot est alors formé de symboles tous différents).

On dit qu'une application est *bijective* (ou une *bijection*) si elle est à la fois injective et surjective. (Le rangement contient alors un objet et un seul dans chaque case ; le mot contient tous les symboles une fois et une fois seulement : c'est une « permutation » des n symboles).

Exemple. $X = \{ 1, 2, ..., 7 \}$, $A = \{ a, b, c, d, e \}$.

L'application :

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ a & c & e & a & e & b & d \end{pmatrix} = aceaebd$$

est surjective, ce qui implique $| X | \geqslant | A |$.

Si $X = \{ 1, 2, 3 \}$, $A = \{ a, b, c, d, e \}$, l'application

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ d & b & e \end{pmatrix} = dbe$$

est injective, ce qui implique $| X | \leqslant | A |$.

Notons que les applications de X dans A *avec un domaine de valeurs aussi étendu que possible sont nécessairement* :

injectives si	$\| X \| < \| A \|$,
bijectives si	$\| X \| = \| A \|$,
surjectives si	$\| X \| > \| A \|$.

Pour montrer que deux ensembles ont le même nombre d'éléments, une façon simple sera de définir une bijection entre ces ensembles.

§ 2. *La cardinalité du produit cartésien* $A \times X$

A partir de maintenant, nous considérons un ensemble A de m éléments notés $a_1, a_2, ..., a_m$ et un ensemble X de n éléments notés 1, 2, ..., n.

$m \times n$ est donc *le nombre d'éléments* de $A \times X$, ce que l'on peut énoncer :

PROPOSITION 1. *On a* : $| A \times X | = | A | \times | X |$.

APPLICATION (Erdös, Szekeres [1]). *Montrer que dans une séquence de* $mn + 1$ *entiers distincts* $u_1, u_2, ..., u_{mn+1}$, *il existe ou bien une séquence partielle décroissante de longueur* $> m$ *ou bien une séquence partielle croissante longueur* $> n$.

Posons : l_i^- = longueur de la plus longue suite partielle décroissante commençant par le terme u_i ;

l_i^+ = longueur de la plus longue suite partielle croissante commençant par le terme u_i.

Supposons que la proposition soit fausse.

$u_i \to (l_i^-, l_i^+)$ définit une application de $\{ u_1, ..., u_{mn+1} \}$ dans le produit cartésien $\{ 1, 2, ..., m \} \times \{ 1, 2, ..., n \}$; cette application est injective, car, si $i < j$, on a

$$u_i > u_j \Rightarrow l_i^- > l_j^- \Rightarrow (l_i^-, l_i^+) \neq (l_j^-, l_j^+) ,$$

$$u_i < u_j \Rightarrow l_i^+ > l_j^+ \Rightarrow (l_i^-, l_i^+) \neq (l_j^-, l_j^+) .$$

On aurait donc, d'après la proposition précédente,

$$mn + 1 \leqslant mn .$$

D'où la contradiction.

Il est à noter que cette propriété a été souvent redécouverte ; elle a été généralisée par C. FRASNAY sous la forme suivante [5] :

Dans une séquence $(u_1, u_2, ...)$ de $n_1 n_2 ... n_p + 1$ éléments distincts, donnons-nous des relations d'ordre total $\overset{1}{<}, \overset{2}{<}, ..., \overset{p}{<}$, telles que les ensembles $R_k = \{ (u_i, u_j) / u_i \overset{k}{<} u_j \}$ recouvrent l'ensemble $\{ (u_i, u_j) / u_i \neq u_j \}$; alors il existe une relation $\overset{k}{<}$ et une suite partielle $(u_{i_1}, u_{i_2}, ...)$ de longueur $n_k + 1$ telle que

$$u_{i_1} \overset{k}{<} u_{i_2} \overset{k}{<} ...$$

Ceci se démontre de la même façon, en utilisant la relation

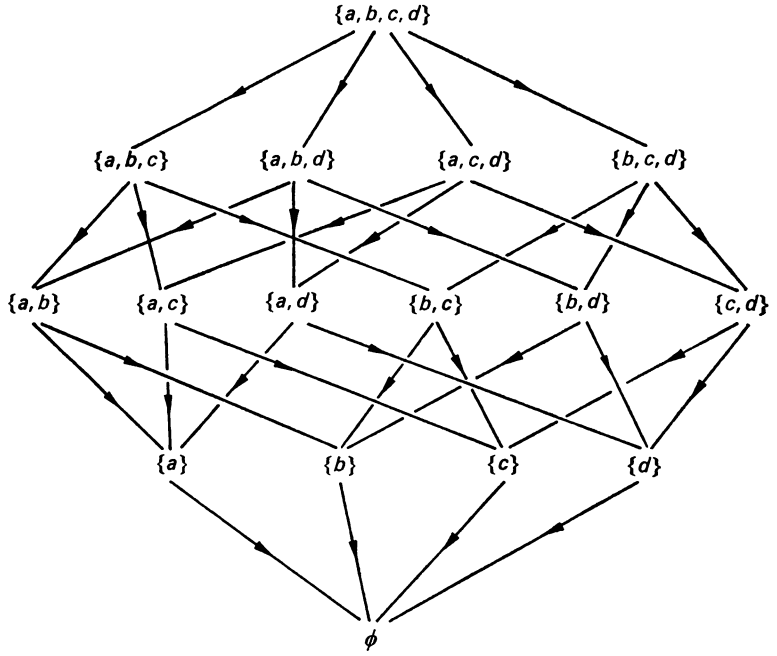
$$| A_1 \times A_2 \times \cdots \times A_p | = | A_1 | \times | A_2 | \times \cdots \times | A_p | .$$

§ 3. *Le nombre de parties d'un ensemble A à m éléments*

Nous nous proposons de dénombrer les sous-ensembles de l'ensemble $A = \{ a_1, a_2, ..., a_m \}$, c'est-à-dire de chercher $| \mathscr{P}(A) |$.

Exemple. $A = \{ a, b, c, d \}$.

Les sous-ensembles de A sont donnés par le tableau suivant :



Dans cette figure, on a tracé un arc allant de l'ensemble S à l'ensemble T si

1° $S \supset T$

2° $S \supset R \supset T$ *entraîne* $R = S$ ou $R = T$.

Comme toutes les flèches sont descendantes, on omet en général de les dessiner.

On sait que la relation $\supset$ est une relation d'ordre, c'est-à-dire

1° $S \supset S$,

2° $S \supset T$, $T \supset S$ *entraîne* $S = T$,

3° $S \supset T$, $T \supset U$ *entraîne* $S \supset U$.

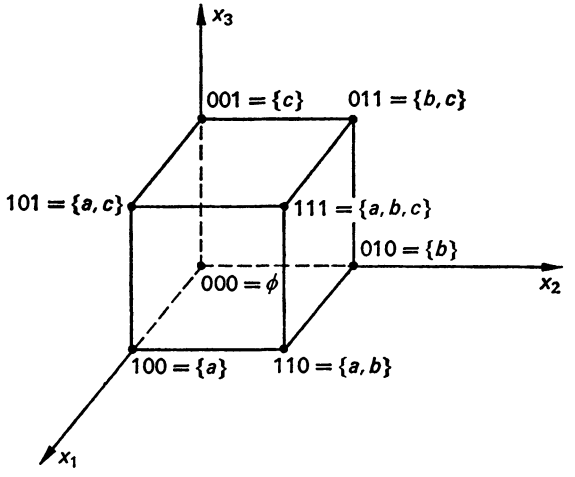
En outre, pour deux éléments S et T, il existe toujours un plus petit majorant $S \cup T$ et un plus grand minorant $S \cap T$. En d'autres termes, $\mathscr{P}(A)$ est un *treillis*.

On remarquera que

$$|\mathscr{P}(A)| = 16 = 2^4 .$$

Remarque. Les parties d'un ensemble à m-éléments seront parfois représentées par les sommets d'un hypercube dans l'espace à m dimensions.

Par exemple, avec $A = \{ a, b, c \}$, on obtient :



Dans cette représentation, les arêtes du cube sont les mêmes que les arêtes dans la représentation précédente. On a ici :

$$| \mathscr{P}(A) | = 8 = 2^3 .$$

PROPOSITION. *Le nombre des parties d'un ensemble A à m éléments est* :

$$| \mathscr{P}(A) | = 2^m$$

(évident).

§ 4. *Les nombres m^n ou les applications de X dans A*

Considérons un ensemble A de m éléments, et le produit cartésien

$$A \times A \times \cdots \times A = A^n ;$$

c'est l'ensemble de tous les *n-uples* $a_1, a_2, ..., a_n$, avec $a_1, a_2, ..., a_n \in A$.

Exemple. Quels sont les 4-uples que l'on peut former avec les lettres a et b ? Ce sont :

aaaa	*abaa*	*baaa*	*bbaa*
aaab	*abab*	*baab*	*bbab*
aaba	*abba*	*baba*	*bbba*
aabb	*abbb*	*babb*	*bbbb*

Il y en a $16 = 2^4$.

PROPOSITION. *m^n est le nombre de n-uples formés avec m symboles.*

En effet, un n-uple contient n symboles ; on a m possibilités pour le premier symbole ; m possibilités pour le deuxième symbole ; etc. Le nombre de n-uples est donc $m \times m \times \cdots \times m = m^n$.

PROPOSITION ÉQUIVALENTE. *m^n est le nombre d'applications d'un ensemble X de n éléments dans un ensemble A de m éléments.*

Evident, avec la correspondance :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_{i_1} & a_{i_2} & & a_{i_n} \end{pmatrix} \to a_{i_1}\, a_{i_2} \dots a_{i_n}\,.$$

§ 5. *Les nombres $[m]_n$ ou les injections de X dans A*

Si x est un nombre réel, on posera à partir de maintenant :

$$[x]_n = \underbrace{x(x-1)\,(x-2) \dots (x-n+1)}_{n}\,.$$

Soient m et n deux entiers, avec $m \geqslant n$; nous allons dénombrer les n-uples pris dans un ensemble A de cardinalité m, et ne présentant pas de répétitions de symboles.

Exemple. $A = \{ a, b, c, d \}$.

Avec $m = 4$, $n = 2$ on trouve douze paires :

$$\left.\begin{array}{cccc} ab & ba & ca & da \\ ac & bc & cb & db \\ ad & bd & cd & dc \end{array}\right\} (T_2)\,.$$

PROPOSITION. *$[m]_n$ est le nombre de n-uples sans répétitions formés avec m symboles.*

Supposons formé le tableau T_{n-1} de tous les $(n-1)$-uples sans répétitions ; on va former un tableau T_n en prenant chaque mot de T_{n-1} et en lui ajoutant au bout, successivement, chacun des $(m-n+1)$ symboles qui n'y figurent pas.

On obtient ainsi le tableau de tous les n-uples sans répétitions car :

1° Ce sont des n-uples sans répétitions,

2° Il n'y a pas d'omission ; le n-uple $\alpha_1\, \alpha_2 \dots \alpha_n$ figure dans T_n puisque $\alpha_1\, \alpha_2 \dots \alpha_{n-1}$ figure nécessairement dans T_{n-1} ;

3° Il n'y a pas de répétitions, car deux n-uples de T_n ou bien diffèrent par les $(n-1)$ premiers symboles, s'ils proviennent de $(n-1)$-uples différents, ou par le n-ième symbole s'ils proviennent du même $(n-1)$-uple.

D'autre part, on a

$$\begin{aligned} |T_n| &= (m-n+1)\,|T_{n-1}|\,, \\ &= (m-n+1)(m-n+2)\ldots(m-1)\,|T_1|\,, \\ &= (m-n+1)(m-n+2)\ldots(m-1)\,m = [m]_n\,. \end{aligned}$$

PROPOSITION. *$[m]_n$ est le nombre d'injections d'un ensemble X de n éléments dans un ensemble A de m éléments.*

En effet, un n-uple sans répétitions, tel que *adcb*, correspond à une application injective telle que

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & d & c & b \end{pmatrix}.$$

m ! ou « factorielle m »

Il est d'usage de poser :

$$m! = \begin{cases} 1 \times 2 \times \cdots \times m & \text{si } m \text{ entier} > 0 \\ 1 & \text{si } m = 0 \end{cases}$$

m ! est donc le nombre de permutations de m objets $a_1, a_2, \ldots, a_m$, c'est-à-dire le nombre de façons de ranger m objets distincts dans m places données.
On peut ainsi écrire

$$[m]_n = \frac{m(m-1)\ldots(m-n+1)(m-n)\ldots 1}{(m-n)\ldots 1} = \frac{m!}{(m-n)!}\,.$$

Nombres de Stirling de première espèce

Le polynôme $[x]_n$, étant un polynôme de degré n, peut s'écrire sous la forme :

$$\boxed{[x]_n = s_n^0 + s_n^1\,x + s_n^2\,x^2 + \cdots + s_n^n\,x^n}\,.$$

Les coefficients s_n^k sont par définition les *nombres de Stirling de première espèce.*

Relations de récurrence

Pour calculer les nombres de Stirling de première espèce, on a les formules suivantes :

$$\boxed{\begin{aligned} s_{n+1}^k &= s_n^{k-1} - n s_n^k\,, \\ s_n^0 &= 0\,, \\ s_n^n &= 1\,. \end{aligned}}$$

En effet, on a

$$[x]_{n+1} = \cdots + s_{n+1}^{k}\, x^k + \cdots = [x]_n\,(x - n)$$
$$= (\cdots + s_n^{k-1}\, x^{k-1} + s_n^k\, x^k + \cdots)\,(x - n).$$

Identifions les coefficients de x^k dans le terme de gauche et celui de droite : on obtient la première des formules annoncées. Les autres sont immédiates.

On trouvera ainsi, de proche en proche, les valeurs suivantes :

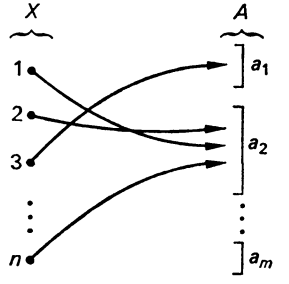
s_n^k	$k = 0$	1	2	3	4 ...
$n = 1$	0	1	0	0	0 ...
2	0	− 1	1	0	0 ...
3	0	2	− 3	1	0 ...
4	0	− 6	11	− 6	1 ...

§ 6. *Les nombres* $[m]^n$

Si x est un nombre réel, on désignera dorénavant par $[x]^n$ le polynôme

$$[x]^n = x(x + 1)\,(x + 2) \ldots (x + n - 1)\,.$$

Supposons que X soit un ensemble de n objets $1, 2, \ldots, n$ que l'on veut ranger dans des boîtes données ; chaque boîte peut contenir autant d'objets qu'on veut, mais s'il y a plusieurs objets dans la même boîte ils se trouvent placés dans un certain ordre (« boîtes ordonnées »).



On se propose de chercher le nombre de rangements de n objets en m boîtes ordonnées.

Exemple. Considérons les rangements dans deux boîtes ordonnées ; par exemple, celui où les objets *ijk* sont dans la première boîte dans cet ordre et l'objet *l* dans la seconde boîte se notera : *ijk* / *l* ; on trouve les rangements suivants avec $X = \{1, 2\}$

$$\begin{cases} \varnothing / 12 & 1 / 2 & 12 / \varnothing \\ \varnothing / 21 & 2 / 1 & 21 / \varnothing \end{cases}$$

PROPOSITION. *Le nombre de façons de ranger n objets dans m boîtes ordonnées est* $[m]^n$.

Supposons formé le tableau T_{n-1} de tous les rangements des objets 1, 2, ..., $n-1$ dans les m boîtes données. Chaque rangement

$$i_1\, i_2 \ldots / \, i_k\, i_{k+1} \ldots / \ldots / \ldots i_{n-1}$$

peut se noter par une suite de $(n-1)+(m-1)$ symboles (lettres ou barres) ; on peut lui ajouter le symbole n de $(n-1)+(m-1)+1$ façons différentes.

Donc

$$|\, T_n \,| = (m+n-1)\,|\, T_{n-1} \,| = (m+n-1)(m+n-2) \ldots (m+1)\,|\, T_1 \,| = [m]^n$$

§ 7. *Les nombres* $\dfrac{[m]^n}{n!}$, *ou les applications croissantes de X dans A*

Soit A un ensemble de symboles $a_1, a_2, \ldots, a_m$, que l'on suppose ordonné dans cet ordre :

$$a_1 < a_2 < a_3 < \cdots < a_m .$$

Un mot $x_1\, x_2 \ldots x_n$ de longueur n sera *croissant* si

$$x_1 \leqslant x_2 \leqslant x_3 \leqslant \cdots \leqslant x_n .$$

Exemple. A est l'ensemble $\{abcd\}$ ordonné dans cet ordre. Les mots croissants de longueur 3 formés avec A sont :

aaa	*abb*	*acc*	*add*
aab	*abc*	*acd*	
aac	*abd*		
aad			
bbb	*bcc*	*bdd*	
bbc	*bcd*		
bbd			
ccc	*cdd*		
ccd			
ddd			

Il y en a 20.

(Dans l'ancienne terminologie, les éléments ci-dessus sont appelés « combinaisons avec répétition de m objets pris n à n ».)

PROPOSITION. *Le nombre de mots croissants de longueur n formés avec m symboles est* $\dfrac{[m]^n}{n!}$.

En effet, considérons un rangement de n objets 1, 2, ..., n dans m boîtes ordonnées a_1, a_2, ..., a_m, comme au paragraphe précédent, et faisons-lui correspondre un mot croissant de la façon suivante :

$$\underbrace{|\ 3\ |}_{a_1}\quad \underbrace{|\ 251\ |}_{a_2}\quad \underbrace{|\ \ |}_{a_3}\quad \underbrace{|\ 647\ |}_{a_4}\quad \rightarrow\quad a_1a_2a_2a_2a_4a_4a_4$$

On écrit le symbole a_1 autant de fois qu'il y a d'objets dans la liste a_1, puis le symbole a_2 autant de fois qu'il y a d'objets dans la liste a_2, etc.

A chaque rangement de n objets correspond un mot croissant et un seul ; un mot croissant peut provenir de $n!$ rangements distincts. D'après la formule du paragraphe précédent, le nombre de mot croissants est donc $\dfrac{[m]^n}{n!}$.

PROPOSITION ÉQUIVALENTE. $\dfrac{[m]^n}{n!}$ *est le nombre d'applications croissantes de X dans A.*

Application (De Moivre). Cherchons le nombre d'additions réalisant le total $m = u_1 + u_2 + \cdots + u_n$ avec n entiers positifs ou nuls, deux additions différant par la nature des entiers employés ou par leur ordre.

Posons $s_k = u_1 + u_2 + \cdots + u_k$. Chaque addition est définie par un mot $s_1\, s_2 \ldots s_{n-1}$, avec

$$0 \leqslant s_1 \leqslant s_2 \leqslant \cdots \leqslant s_{n-1} \leqslant m\,.$$

La réponse est donc

$$\frac{[m+1]^{n-1}}{(n-1)!} = \frac{(m+n-1)!}{(n-1)!\,m!}\,.$$

8. *Les nombres binomiaux*

Cherchons le nombre de parties à n éléments d'un ensemble A de cardinalité m.

Exemple. $A = \{a, b, c, d, e\}$, $n = 3$. On trouve :

abc	*acd*	*ade*
abd	*ace*	
abe		
bcd	*bde*	
bce		
cde		

On obtient 10 sous-ensembles de A à 3 éléments. On peut aussi considérer ce tableau comme la liste des mots *strictement croissants.*

PROPOSITION. *Le nombre de sous-ensembles de A à n éléments est* :

$$\frac{[m]_n}{n!} = \frac{m(m-1)(m-2)\ldots(m-n+1)}{1.2.\ldots.n} = \frac{m!}{n!(m-n)!}.$$

Supposons formé le tableau T des n-uples strictement croissants pris dans un ensemble A de m objets ; on permute les lettres dans chacun de ces n-uples de toutes les façons possibles, et on porte les résultats dans un tableau T'.

On obtient ainsi le tableau des n-uples sans répétitions pris dans A. Il n'y a pas d'omission : tout n-uple d'objets distincts figure dans T'.

Il n'y a pas de répétition, car deux n-uples de T' proviennent soit d'un même n-uple de T — et alors ils diffèrent par l'ordre des lettres — soit de deux n-uples différents de T — et alors ils diffèrent par la nature des lettres.

D'après le § 6, le tableau T' a $[m]_n$ éléments, donc le tableau T a $\dfrac{[m]_n}{n!}$ éléments. C. Q. F. D.

Il est d'usage de poser :

$$\binom{m}{n} = \begin{cases} \dfrac{[m]_n}{n!} & \text{si } n \neq 0,\ m \geqslant n \\ 1 & \text{si } n = 0,\ m \geqslant n \\ 0 & \text{si } m < n \end{cases}.$$

Ce nombre $\binom{m}{n}$ s'appelle *le nombre binomial en m et n.* Dans l'ancienne terminologie, il était appelé le « nombre de combinaisons de m objets pris n à n» ; on le notera aussi parfois C_m^n. (A noter que l'indice supérieur dans un des symboles est l'indice inférieur dans l'autre.)

Formule 1. On a pour $m \geqslant n > 0$:

$$\boxed{\begin{aligned} &\binom{m}{n} = \binom{m-1}{n} + \binom{m-1}{n-1} \\ &\binom{m}{0} = \binom{m}{m} = 1 \end{aligned}}$$

En effet, formons le tableau T des n-uples strictement croissants pris dans $A = \{a_1, \ldots, a_m\}$; on peut le diviser en deux tableaux, l'un T' des n-uples, contenant a_1, l'autre T'' des n-uples ne contenant pas a_1. T' est sans omission

ni répétition, le tableau des $(n-1)$-uples pris dans $\{a_2, a_3, ..., a_m\}$, et T'' celui des n-uples pris dans $\{a_2, a_3, ..., a_m\}$; d'où la première de ces égalités. Les deux autres sont immédiates.

Remarque. — On déduit de la formule 1 une loi de récurrence permettant de déterminer tous les $\binom{m}{n}$ de proche en proche, ce qui donne :

$\binom{m}{n}$	$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	...
$m=1$	1	1	0	0	0	0	...
$m=2$	1	2	1	0	0	0	...
$m=3$	1	3	3	1	0	0	...
$m=4$	1	4	6	4	1	0	...
$m=5$	1	5	10	10	5	1	...
...							

Le tableau ainsi formé s'appelle le *triangle de Pascal.* On remarque :

1° Les coefficients équidistants des extrêmes sont égaux, c'est-à-dire

$$\boxed{\binom{m}{n} = \binom{m}{m-n}}.$$

En effet, les deux membres sont égaux à

$$\frac{m!}{n!\,(m-n)!}.$$

2° Pour m fixe, les nombres $\binom{m}{n}$ vont en croissant tant que

$$n \leqslant \frac{m+1}{2}.$$

En effet,

$$\binom{m}{n-1} \leqslant \binom{m}{n}$$

est équivalent à

$$\frac{m!}{(n-1)!\,(m-n+1)!} \leqslant \frac{m!}{n!\,(m-n)!}$$

ou :

$$\frac{1}{m-n+1} \leqslant \frac{1}{n}$$

ou :

$$n \leqslant \frac{m+1}{2}.$$

Formule 2. (Généralisation de la formule 1). On a, pour $m, n, p \geqslant 1$, $m + p \geqslant n$,

$$\boxed{\binom{m+p}{n} = \sum_{k=0}^{m} \binom{m}{k}\binom{p}{n-k}}.$$

Pour $p = 1$, $n \geqslant 1$, on trouve

$$\binom{m+1}{m} = \binom{m}{m-1} + \binom{m}{n}.$$

C'est la formule 1.
Pour $p = 2$, $n \geqslant 2$, on obtient

$$\binom{m+2}{n} = \binom{m}{n-2} + 2\binom{m}{n-1} + \binom{m}{n}.$$

Plus généralement, si $n \geqslant p$, on obtient :

$$(1) \qquad \binom{m+p}{n} = \binom{m}{n-p} + \binom{m}{n-p+1}\binom{p}{p-1} + \binom{m}{n-p+2}\binom{p}{p-2} + \cdots + \binom{m}{n}\binom{p}{0}.$$

Si $n \leqslant p$, on obtient :

$$(2) \qquad \binom{m+p}{n} = \binom{m}{0}\binom{p}{n} + \binom{m}{1}\binom{p}{n-1} + \cdots + \binom{m}{n}\binom{p}{0}.$$

Formons le tableau T des sous-ensembles de $\{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_p\}$ avec n éléments ; en supposant $n \geqslant p$:

— ceux qui contiennent tous les b_i sont en nombre $\binom{m}{n-p}$,

— ceux qui contiennent $p-1$ des b_i sont en nombre $\binom{p}{p-1}\binom{m}{n-p+1}$

— etc.

D'où la formule (1).
Si $n \leqslant p$, on trouve la formule (2).

Formule du binôme dans un anneau commutatif

Considérons un ensemble A muni d'une opération notée $+$ et appelée l'*addition*, avec les axiomes suivants :

1. $a + (b + c) = (a + b) + c = a + b + c$ (associativité) ;
2. $a + b = b + a$ (commutativité) ;
3. Existence d'un élément neutre 0 :
$$0 + a = a$$
4. Existence d'un élément inverse $-a$:
$$a + (-a) = 0$$

A est alors un *groupe abélien* ; supposons que A soit également muni d'une opération, notée ., et appelé la multiplication, avec les axiomes :

5. $a.(b.c) = (a.b).c = a.b.c$ (associativité) ;
6. $a.b = b.a$ (commutativité) ;
7. $a.(b + c) = a.b + a.c$ (distributivité par rapport à l'addition).

On dit alors que A est un *anneau commutatif*.

Exemples. L'ensemble Z des entiers positifs, négatifs ou nuls ; l'ensemble R des nombres nuls, l'ensemble Γ des nombres rationnels, l'ensemble Ω des nombres complexes ; l'ensemble des polynômes ayant leurs coefficients dans Z ; ou dans R ; ou dans Γ ; ou dans Ω ; l'ensemble des fonctions définies et bornées sur l'intervalle [0, 1] ; etc.

Considérons dans A deux n-uples $(a^1, a^2, ..., a^n)$ et $(b^1, b^2, ..., b^n)$, et proposons-nous de développer le produit :

$$(a^1 + b^1)(a^2 + b^2) ... (a^n + b^n) = \prod_{i=1}^{n} (a^i + b^i) .$$

Si $K \subset N = \{1, 2, ..., n\}$, on posera si $|K| = k \neq 0$:

$$a^K = \prod_{i \in K} a^i , \quad b^K = \prod_{i \in K} b^i .$$

Si $k = 0$, on posera arbitrairement $a^\varnothing b^N = b^N$, $a^N b^\varnothing = a^N$; on a :

$$\prod_{i \in N} (a^i + b^i) = (a^1 + b^1)(a^2 + b^2) ... (a^n + b^n) = \sum_{K \subset N} a^K b^{N-K} .$$

Faisons $a^1 = a^2 = \cdots = a^n = a$, $b^1 = b^2 = \cdots = b^n = b$, on obtient :

$$\boxed{(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}} .$$

Application. Considérons dans l'espace vectoriel Φ des fonctions à variables réelles un opérateur linéaire P, c'est-à-dire une loi qui fait correspondre à toute fonction $\varphi \in \Phi$ une fonction $P\varphi \in \Phi$, avec :

$$P[\varphi(x) + \psi(x)] = P\varphi(x) + P\psi(x),$$

$$P[\lambda\varphi(x)] = \lambda P\varphi(x), \quad \lambda = \text{constante}.$$

Si P et Q sont deux opérateurs, on pose

$$(P + Q)\,\varphi(x) = P\varphi(x) + Q\varphi(x),$$

$$(PQ)\,\varphi(x) \quad = P[Q\varphi(x)].$$

Considérons maintenant deux opérateurs P et Q commutatifs (c'est-à-dire : $PQ = QP$) ; l'ensemble des opérateurs, déduits de P et Q par une succession d'additions et de multiplications, forme un anneau commutatif ; on a donc :

$$(P + Q)^n\,\varphi(x) = \sum_{k=0}^{n} \binom{n}{k} P^k\, Q^{n-k}\,\varphi(x).$$

Considérons en particulier les opérateurs :

$$E\varphi(x) = \varphi(x + 1),$$

$$I\varphi(x) = \varphi(x),$$

$$\Delta\varphi(x) = \varphi(x + 1) - \varphi(x) = (E - I)\,\varphi(x).$$

On peut écrire

$$\Delta^n\,\varphi(x) = (E - I)^n\,\varphi(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} E^k\,\varphi(x).$$

D'où finalement la formule bien souvent utilisée :

$$\boxed{\Delta^n\,\varphi(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \varphi(x + k)}\ .$$

Nombres de Fibonacci

1° Proposons-nous de chercher le nombre $f(n, k)$ des sous-ensembles de $X = \{1, 2, ..., n\}$, qui ont k éléments, et ne contiennent pas deux entiers consécutifs.

A un tel sous-ensemble S, on peut faire correspondre un mot $\alpha_1\,\alpha_2\,...\,\alpha_n$, avec

$$\alpha_i = \begin{cases} 0 & \text{si} \quad i \notin S \\ 1 & \text{si} \quad i \in S. \end{cases}$$

Ce mot, formé de 0 et de 1, n'aura pas deux 1 adjacents. L'application entre de tels sous-ensembles S et de tels mots $\alpha_1 \alpha_2 \ldots \alpha_n$ est bijective ; on se contentera donc de dénombrer les mots.

Considérons $n - k$ chiffres 0, numérotés de 1 à $n - k$, et ajoutons k chiffres 1 de façon qu'il n'y en ait pas deux adjacents ; chaque 1 peut être caractérisé par le numéro d'ordre du 0 qui le précède : il faut donc choisir k entiers dans l'ensemble $\{ 0, 1, 2, \ldots, n - k \}$, ce qui représente un nombre de possibilités égal à

$$f(n, k) = \binom{n - k + 1}{k}.$$

Le nombre de sous-ensembles de X qui ne contiennent pas deux entiers consécutifs est donc

$$F_n = \sum_k \binom{n - k + 1}{k}.$$

Ces nombres F_n s'appellent *les nombres de Fibonacci.*

2° Proposons-nous de chercher le nombre $f^*(n, k)$ des sous-ensembles de X, à k éléments, et ne contenant ni deux entiers consécutifs, ni les chiffres 1 et n simultanément.

Les sous-ensembles qui contiennent le chiffre n ne peuvent contenir ni $n - 1$, ni 1, et sont donc en nombre $f(n - 3, k - 1)$; ceux qui ne contiennent pas le chiffre n sont en nombre $f(n - 1, k)$. D'où

$$\begin{aligned} f^*(n, k) &= f(n - 3, k - 1) + f(n - 1, k) \\ &= \binom{n - k - 1}{k - 1} + \binom{n - k}{k} \\ &= \binom{n - k}{k} \left[\frac{k}{n - k} + 1 \right] \\ &= \frac{n}{n - k} \binom{n - k}{k}. \end{aligned}$$

Le nombre de sous-ensembles de X qui ne contiennent pas deux chiffres consécutifs modulo $(n - 1)$ est donc

$$F_n^* = \sum_k \frac{n}{n - k} \binom{n - k}{k}.$$

Ces nombres F_n^* sont parfois appelés les *nombres de Fibonacci corrigés.*

§ 9. *Les nombres multinomiaux* $\binom{n}{n_1, n_2, \cdots, n_p}$

PROPOSITION. *Soit X un ensemble de n objets et $n_1, n_2, \ldots, n_p$ des entiers positifs ou nuls avec $n_1 + n_2 + \cdots + n_p = n$; le nombre de rangements des objets dans des boîtes $X_1, X_2, \ldots, X_p$, contenant respectivement $n_1, n_2, \ldots, n_p$ objets est :*

$$\binom{n}{n_1, n_2, \ldots, n_p} = \begin{cases} \dfrac{n!}{n_1!\, n_2! \ldots n_p!} & \text{si} \quad n_1 + n_2 + \cdots + n_p = n \\ 0 & \text{sinon .} \end{cases}$$

Supposons $n_1 + n_2 + \cdots + n_p = n$.

L'ensemble X_1 peut être choisi de $\binom{n}{n_1}$ façons différentes ; en supposant l'ensemble X_1 fixé, X_2 peut être choisi ensuite de $\binom{n - n_1}{n_2}$ façons différentes, etc.

Le nombre cherché est donc

$$\binom{n}{n_1}\binom{n - n_1}{n_2}\binom{n - n_1 - n_2}{n_3} \cdots \binom{n_p}{n_p} =$$

$$= \frac{n!}{n_1!\,(n - n_1)!} \frac{(n - n_1)!}{n_2!\,(n - n_1 - n_2)!} \frac{(n - n_1 - n_2)!}{n_3!\,(n - n_1 - n_2 - n_3)!} \cdots \frac{n_p!}{n_p!}$$

$$= \frac{n!}{n_1!\, n_2!\, n_3! \ldots n_p!} .$$

Formule du multinôme dans un anneau commutatif

Si A est un anneau commutatif (cf. § 8), *et si $a_1, a_2, \ldots, a_p \in A$ on a :*

$$\boxed{(a_1 + a_2 + \cdots + a_p)^n = \sum_{\substack{n_1, n_2, \ldots, n_p \geqslant 0 \\ n_1 + n_2 + \ldots + n_p = n}} \binom{n}{n_1, n_2, \ldots, n_p} a_1^{n_1} a_2^{n_2} \ldots a_p^{n_p}} .$$

En effet, considérons des éléments $a_j^i \in A$ et formons le produit :

$$(a_1^1 + a_2^1 + \cdots + a_p^1)(a_1^2 + a_2^2 + \cdots + a_p^2) \ldots (a_1^n + a_2^n + \cdots + a_p^n) .$$

Des nombres $n_1, n_2, \ldots, n_p$ positifs ou nuls étant donnés (avec $n_1 + n_2 + \cdots + n_p = n$), considérons chaque monôme de la forme :

$$(a_1^{i_1} a_1^{i_2} \ldots a_1^{i_{n_1}})(a_2^{j_1} a_2^{j_2} \ldots a_2^{j_{n_2}}) \ldots (a_p^{k_1} a_p^{k_2} \ldots a_p^{k_{n_p}})$$

il lui correspond bi-univoquement un rangement de l'ensemble $N = \{1, 2, ..., n\}$ dans des boites $N_1, N_2, ..., N_p$, avec $|N_1| = n_1, |N_2| = n_2, ..., |N_p| = n_p$; leur nombre est donc :

$$\binom{n}{n_1, n_2, ..., n_p} = \frac{n!}{n_1!\, n_2! \dots n_p!}.$$

En faisant, pour tout i,

$$a_i^1 = a_i^2 = \cdots = a_i^n = a_i,$$

on obtient la formule annoncée.

CONSÉQUENCE 1. *On a* :

$$\binom{n}{n_1, n_2, ..., n_p} = \sum_{i\,/\,n_i \neq 0} \binom{n-1}{n_1, n_2, ..., n_{i-1}, n_i - 1, n_{i+1}, ..., n_p}.$$

En effet, on a

$$(a_1 + a_2 + \cdots + a_p)^n = (a_1 + a_2 + \cdots + a_p)(a_1 + a_2 + \cdots + a_p)^{n-1}.$$

Le terme général est

$$\binom{n}{n_1, n_2, ..., n_p} a_1^{n_1} a_2^{n_2} \dots a_p^{n_p} = \sum_{i\,/\,n_i \neq 0} a_i \binom{n-1}{n_1, ..., n_i - 1, ..., n_p} a_1^{n_1} \dots a_i^{n_i - 1} \dots a_p^{n_p}.$$

CONSÉQUENCE 2. *On a* :

$$\binom{m+q}{n_1, n_2, ..., n_p} = \sum_{\substack{(k_1, k_2, ...) \leqslant (n_1, n_2, ...) \\ k_1 + k_2 + \cdots = m}} \binom{m}{k_1, k_2, ..., k_p} \binom{q}{n_1 - k_1, n_2 - k_2, ..., n_p - k_p}.$$

En effet, on a

$$(a_1 + a_2 + \cdots + a)^{m+q} = (a_1 + a_2 + \cdots + a_p)^m (a_1 + a_2 + \cdots + a_p)^q.$$

Le terme général est

$$\binom{m+q}{n_1, n_2, ..., n_p} a_1^{n_1} a_2^{n_2} \dots a_p^{n_p} = \sum_{\substack{(k_1, k_2, ...) \leqslant (n_1, n_2, ...) \\ k_1 + k_2 + \cdots + k_p = m}} \binom{m}{k_1, k_2, ..., k_p} \times$$

$$\times\, a_1^{k_1} a_2^{k_2} \dots a_p^{k_p} \binom{q}{n_1 - k_1, n_2 - k_2, ..., n_p - k_p} a_1^{n_1 - k_1} a_2^{n_2 - k_2} \dots a_p^{n_p - k_p}.$$

(Ces formules sont analogues aux formules 1 et 2 des paragraphes précédents, et, comme elles, pourraient aussi se démontrer directement.)

CONSÉQUENCE 3. *On a* :

$$\sum \binom{n}{n_1, n_2, \ldots, n_p} (-1)^{n_2+n_4+n_6+\cdots} = \frac{1-(-1)^p}{2}.$$

Faisons

$$+1 = a_1 = a_3 = a_5 = \cdots$$
$$-1 = a_2 = a_4 = a_6 = \cdots$$

Si p est pair, comme si p est impair, on peut donc écrire :

$$(a_1 + a_2 + \cdots + a_p)^n = \frac{1-(-1)^p}{2}.$$

D'où la formule.

Beaucoup d'autres formules analogues peuvent être obtenues par le même procédé.

Application au treillis des p-uples.

Considérons l'ensemble N^p des p-uples $a = (a_1, a_2, \ldots, a_p)$ où $a_1, a_2, \ldots, a_p$ sont des entiers $\geqslant 0$. Posons

$$b \leqslant a$$

si $b_i \leqslant a_i$ pour $i = 1, 2, \ldots, p$.

La relation $a \leqslant b$ est une *relation d'ordre*, c'est-à-dire vérifie :

1° $a \leqslant a$,

2° $a \leqslant b$, $b \leqslant a$ *entraîne* $a = b$,

3° $a \leqslant b$, $b \leqslant c$ *entraîne* $a \leqslant c$.

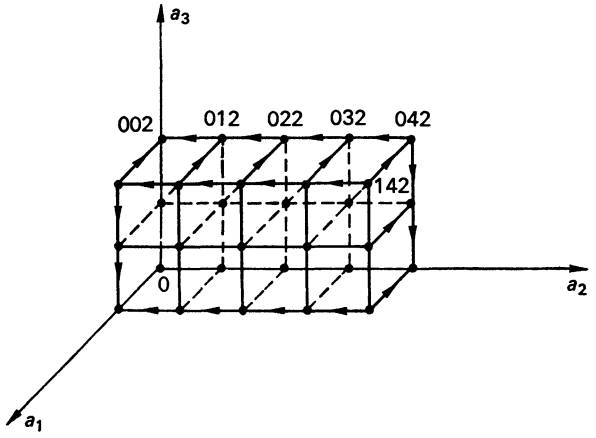
On pose

$$a \vee b = (\max\{a_1, b_1\}, \max\{a_2, b_2\}, \ldots \max\{a_p, b_p\}),$$
$$a \wedge b = (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \ldots \min\{a_p, b_p\}).$$

On remarque alors que l'ensemble ordonné N^p est un treillis, c'est-à-dire que pour deux p-uples a et b, il existe dans N^p un majorant $a \vee b$ plus petit que les autres, et un minorant $a \wedge b$ plus grand que les autres.

Représentons ce treillis par un graphe, dont les sommets sont les p-uples, et l'on joint deux sommets a et b par une flèche allant de a vers b si, pour un i, on a

$$a_k = \begin{cases} b_k & \text{si} \quad k \neq i \\ b_i + 1 & \text{si} \quad k = i. \end{cases}$$



Si $a \geqslant b$, proposons-nous de chercher le nombre de chemins (suivant l'orientation des flèches) allant de a vers b. Par exemple, si $p = 3$, on trouve 10 chemins pour aller de 032 à 000 :

032	022, 012, 002, 001	000
	022, 012, 011, 001	
	022, 012, 011, 010	
	022, 021, 011, 001	
	022, 021, 011, 010	
	022, 021, 020, 010	
	031, 021, 011, 001	
	031, 021, 011, 010	
	031, 021, 020, 010	
	031, 030, 020, 210	

PROPOSITION. *Si $a \geqslant b$, le nombre de chemins allant de a à b est*

$$\binom{\sum (a_i - b_i)}{a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n}.$$

Posons $a_i - b_i = n_i$, $\sum(a_i - b_i) = n$, et appelons α_i l'opération :

$$\alpha_i(a) = (a_1, a_2, \ldots, a_i - 1, a_{i+1}, \ldots, a_n).$$

A tout chemin allant de a vers b faisons correspondre la suite des opérations α_i qui sont effectuées lorsque l'on suit le chemin. On définit ainsi une bijection entre les chemins allant de a à b, et les n-uples contenant n_1 fois le symbole α_1, n_2 fois le symbole α_2, etc. Un tel n-uple $x_1\, x_2 \ldots x_n$ définit un rangement de 1, 2, ..., n dans des boîtes :

$$A_k = \{\, i \,/\, x_i = \alpha_k \,\}.$$

Par exemple, $\alpha_1\,\alpha_1\,\alpha_3\,\alpha_2\,\alpha_3\,\alpha_3$ donne le rangement de 1, 2, ..., 6 dans trois boîtes :

$$A_1 = \{1, 2\}, \qquad A_2 = \{4\}, \qquad A_3 = \{3, 5, 6\};$$

la correspondance est bi-univoque.

Donc le nombre de chemins cherché est

$$\binom{n}{n_1, n_2, \ldots, n_p}$$

§ 10. *Les nombres de Stirling S_n^m, ou les partitions de n objets en m classes*

Considérons un ensemble X; des sous-ensembles $A_1, A_2, \ldots, A_p$ forment une *partition en classes de l'ensemble* X si l'on a :

$$A_i \neq \varnothing,$$
$$i \neq j \text{ entraîne } A_i \cap A_j = \varnothing,$$
$$A_1 \cup A_2 \cdots \cup A_p = X.$$

Les ensembles A_i sont les *classes* de la partition. On reconnaîtra le plus souvent que les ensembles A_i forment une partition d'un ensemble X en vérifiant que la relation « a et b sont contenus dans un même sous-ensemble », ou $a \sim b$, satisfait aux axiomes :

$$a \sim a \qquad \text{(réflexivité)},$$
$$a \sim b \;\Rightarrow\; b \sim a \qquad \text{(symétrie)},$$
$$a \sim b,\ b \sim c \;\Rightarrow\; a \sim c \qquad \text{(transitivité)}.$$

On dit que $\sim$ est une *relation d'équivalence*, et que les A_i sont les classes de cette équivalence.

Considérons une partition $\mathscr{A} = (A_1, A_2, \ldots, A_p)$, qui comporte

λ_1 classes de cardinalité 1,
λ_2 classes de cardinalité 2,
λ_3 classes de cardinalité 3,
...
λ_k classes de cardinalité k.

On dit alors que la partition est *du type*

$$\underbrace{1 + 1 + \cdots + 1}_{\lambda_1} + \underbrace{2 + 2}_{\lambda_2} + \cdots + \underbrace{k + k + \cdots + k}_{\lambda_k}.$$

Pour avoir une expression plus condensée on note parfois ce type en remplaçant les additions par des multiplications, soit :

$$1^{\lambda_1} 2^{\lambda_2} \dots k^{\lambda_k} .$$

Les deux notations seront utilisées par la suite.
Considérons par exemple une collection d'objets hétéroclites dont

5 sont rouges
5 sont verts
2 sont bleus
2 sont jaunes
2 sont noirs
1 est orange.

La couleur définit alors une partition du type $1 + 2 + 2 + 2 + 5 + 5$ (première notation) ou du type $1.2^3.5^2$ (deuxième notation).

Remarque. Parfois, on considère un partage de l'ensemble X en sous-ensembles $A_1, A_2, \dots, A_p$, avec seulement les axiomes

$$i \neq j \quad \Rightarrow \quad A_i \cap A_j = \varnothing ,$$

$$\bigcup_{i=1}^{k} A_i = X .$$

Si les A_i peuvent être vides, on ne parlera pas de « partition en classes », mais de « division en parties » de l'ensemble X. Une « classe » est nécessairement non vide.

Considérons deux partitions $\mathscr{A} = (A_1, A_2, \dots, A_p)$ et $\mathscr{B} = (B_1, B_2, \dots, B_q)$. On pose $\mathscr{A} \prec \mathscr{B}$ si

$$A_i \cap B_j \neq \varnothing \quad \Rightarrow \quad A_i \subset B_j .$$

La relation $\prec$ est une relation d'ordre, c'est-à-dire avec les axiomes :

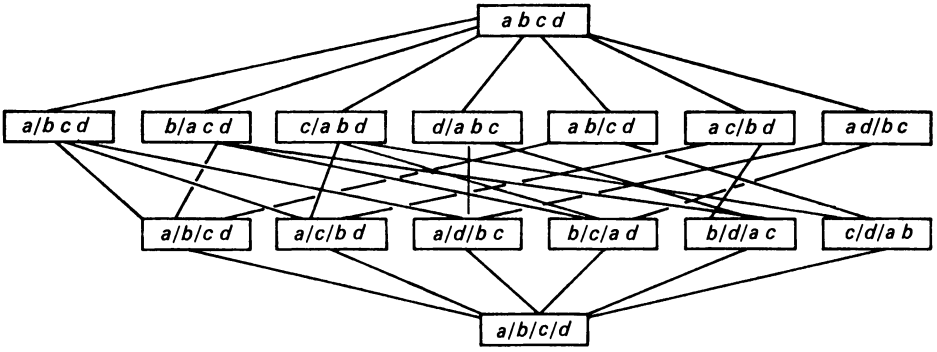
$$\mathscr{A} \prec \mathscr{A}$$
$$\mathscr{A} \prec \mathscr{B}, \quad \mathscr{B} \prec \mathscr{A} \quad \Rightarrow \quad \mathscr{A} = \mathscr{B}$$
$$\mathscr{A} \prec \mathscr{B}, \quad \mathscr{B} \prec \mathscr{C} \quad \Rightarrow \quad \mathscr{A} \prec \mathscr{C} .$$

La vérification est immédiate.

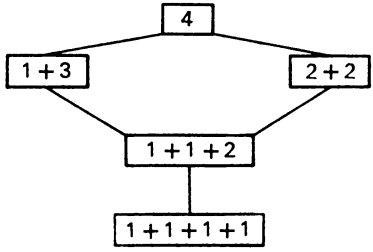
L'ensemble des partitions avec la relation $\prec$ est un treillis, c'est-à-dire que pour deux partitions $\mathscr{A}$ et $\mathscr{B}$, il existe un majorant plus petit que les autres, et il existe un minorant plus grand que les autres.

Exemple. $X = \{a, b, c, d\}$.

On obtient le treillis suivant :



Les types correspondants aux différentes partitions de ce tableau sont :



Il y a donc une relation d'ordre naturelle sur les types de partitions, mais l'on n'a pas un treillis : par exemple, les deux partages $1 + 1 + 3$ et $1 + 2 + 2$ admettent deux majorants $1 + 4$ et $2 + 3$, aucun des deux n'étant plus petit que l'autre.

PROPOSITION 1. *Si X est un ensemble de n objets, le nombre de partitions du type $1^{\lambda_1} 2^{\lambda_2} \dots k^{\lambda_k}$ est égal à :*

$$\frac{n!}{(1!)^{\lambda_1}(2!)^{\lambda_2} \dots (k!)^{\lambda_k}(\lambda_1!)\,(\lambda_2!)\,(\lambda_k!)}.$$

(Immédiat, d'après la proposition du § 9.)

Exemple. $X = \{a, b, c, d\}$. On voit sur la figure que les partitions du type $1^2.2$ sont au nombre de

$$6 = \frac{4!}{(1!)^2(2!)^1(2!)}.$$

Si $n \geqslant m$, on appelle *nombre de Stirling (de deuxième espèce)* le nombre S_n^m de partitions d'un ensemble de n objets en m classes. C'est par exemple le nombre de façons distinctes de ranger un ensemble de n objets distincts dans une collection de m boîtes identiques, sans laisser des boîtes vides (si l'on avait le droit de laisser des boîtes vides, la réponse serait $S_n^1 + S_n^2 + \cdots + S_n^m$).

Exemple. On a 4 objets a, b, c, d. Les partitions en 2 classes sont au nombre de 7, ainsi qu'on peut le voir sur la figure ci-dessus.
Donc $S_4^2 = 7$.

PROPOSITION 2. *$m\,!\,S_n^m$ est le nombre de surjections de X dans A.*

En effet, à toute surjection de $X = \{1, 2, ..., n\}$ dans $A = \{a_1, a_2, ..., a_m\}$ correspond une partition de X en m classes distinctes $a_1, a_2, ..., a_m$; inversement à toute partition de X correspond $m\,!$ surjections de X dans A.

Relations de récurrence

$$\begin{aligned} S_{n+1}^k &= S_n^{k-1} + kS_n^k \quad \text{pour} \quad 1 < k < n, \\ S_n^1 &= S_n^n = 1. \end{aligned}$$

En effet, considérons le tableau des partitions de $n + 1$ objets en k classes.

1° Pour certaines partitions, le $(n + 1)$-ième objet occupe une classe à lui tout seul ; le nombre de ces partitions est S_n^{k-1}.

2° Pour les autres partitions, le $(n + 1)$-ième objet n'est pas seul dans une classe. Il y en a donc kS_n^k, d'où

$$S_{n+1}^k = S_n^{k-1} + kS_n^k.$$

Ces formules permettent de calculer de proche en proche les nombres S_n^k ; on obtient le tableau suivant :

S_n^m	$m = 1$	2	3	4	5	6
$n = 1$	1	0	0	0	0	0
$n = 2$	1	1	0	0	0	0
$n = 3$	1	3	1	0	0	0
$n = 4$	1	7	6	1	0	0
$n = 5$	1	15	25	10	1	0
$n = 6$	1	31	90	65	15	1

C'est le « triangle de Stirling ».

Du triangle de Pascal (§ 8) et du triangle de Stirling, on déduit le tableau des nombres d'applications de X dans A avec un ensemble-image aussi large que possible :

	$m=1$	2	3	4	5	6 ...
$n=1$	1	2	3	4	5	6
2	1	2	6	12	20	30
3	1	6	6	24	60	120
4	1	14	36	24	120	360
5	1	30	150	240	120	720
6	1	62	540	1 560	1 800	720
•						
•						
•						

$n < m$: Le nombre d'injections est $n! \binom{m}{n}$

$n = m$

$n > m$: Le nombre de surjections est $m!\, S_n^m$.

Formule 1. Soit x un nombre réel quelconque, entier ou non ; on a

$$\boxed{x^n = \sum_{k=1}^{n} S_n^k [x]_k} .$$

Soient A et X, avec $|A| = m \leqslant |X| = n$; le nombre d'applications de X dans A est

$$m^n = \sum_{k=1}^{m} \binom{m}{k} (k!\, S_n^k) = \binom{m}{1} 1!\, S_n^1 + \binom{m}{2} 2!\, S_n^2 + \cdots + \binom{m}{n} m!\, S_n^m .$$

L'identité proposée de degré n, étant vraie pour n valeurs de la variable $x = 1, 2, ..., n$, est vraie pour tout x.

Formule 2

$$\boxed{S_{n+1}^m = \sum_{k=0}^{n} \binom{n}{k} S_k^{m-1}} .$$

Considérons le tableau des partitions de $n+1$ objets en m classes.

Supprimons la classe qui contient l'objet $n+1$; on obtient les partitions d'un ensemble d'objets K en $m-1$ classes (pour tout $K \subset \{1, 2, ..., n\}$). D'où la formule.

Exercice. Quel est le nombre de façons de placer n objets distincts dans m boîtes différentes, de façon que k de ces boîtes soient occupées et $m - k$ soient vides ? C'est :

$$(k!\, S_n^k)\binom{m}{k} = S_n^k[m]_k .$$

§ 11. *Le nombre exponentiel de Bell B_n, ou le nombre de partitions en classes de n objets*

On désigne par B_n le nombre total de partitions en classes d'un ensemble X de n objets ; ces nombres sont appelés parfois *nombres exponentiels*, ou *nombres de Bell.*

Exemple. $X = \{ a, b, c, d \}$.

On a 15 partitions, comme on le voit sur la figure de la page 15.
D'où $B_4 = 15$.

Formule 1

$$\boxed{B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k} .$$

On a évidemment, d'après la définition de nombres de Stirling (§ 10),

$$B_n = S_n^1 + S_n^2 + \cdots + S_n^n .$$

Si $m > n$, on posera $S_n^m = 0$; on peut donc écrire, avec la formule 2 (§ 10) :

$$B_{n+1} = \sum_{m=1}^{\infty} S_{n+1}^m = \sum_{m=1}^{\infty} \sum_{k=0}^{n} \binom{n}{k} S_k^{m-1} = \sum_{k=0}^{n} \binom{n}{k} \left(\sum_{m=1}^{\infty} S_k^{m-1} \right) .$$

D'où la formule.

Formule 2 (E. T. BELL)

$$\boxed{\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n = e^{(e^t - 1)}} .$$

Un procédé élégant de démonstration, dû à G. C. ROTA [7], est le suivant.

Considérons l'espace vectoriel des fonctions $\varphi(x)$ telles que

$$\varphi(x) = \sum_{n=0}^{\infty} \alpha_n [x]_n , \qquad \sum_{n=0}^{\infty} |\alpha_n| < +\infty .$$

La fonctionnelle $L(\varphi) = \sum_{n=0}^{\infty} \alpha_n$ est continue et linéaire, car

$$L(\lambda\varphi + \lambda'\varphi') = \sum_{n=0}^{\infty} (\lambda\alpha_n + \lambda'\alpha'_n) = \lambda \sum_{n=0}^{\infty} \alpha_n + \lambda' \sum_{n=0}^{\infty} \alpha'_n .$$

D'autre part, la formule 1 (§ 10) donne

$$L(x^n) = L\left(\sum_{k=1}^{n} S_n^k [x]_k\right) = \sum_{k=1}^{n} S_n^k = B_n .$$

D'où

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n = \sum_{n=0}^{\infty} \frac{L(x^n)}{n!} t^n = L(e^{tx}) .$$

Posons $e^t = (1 + u)$, il vient :

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n = L((1+u)^x) = L\left(\sum_{n=0}^{\infty} \frac{[x]_n}{n!} u^n\right)$$

$$= \sum_{n=0}^{\infty} \frac{u^n}{n!} L([x]_n) = \sum_{n=0}^{\infty} \frac{u^n}{n!} = e^u = e^{(e^t - 1)} .$$

Formule 3 (G. DOBINSKI).

$$\boxed{B_{n+1} = \frac{1}{e}\left(1^n + \frac{2^n}{1!} + \frac{3^n}{2!} + \frac{4^n}{3!} + \cdots\right)} .$$

On a

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \sum_{k=n}^{\infty} \frac{1}{(k-n)!} = \sum_{k=n}^{\infty} \frac{[k]_n}{k!} = \sum_{k=0}^{\infty} \frac{[k]_n}{k!} .$$

La fonctionnelle L, définie pour la formule 2 précédente, vérifie

$$L([x]_n) = 1 = \frac{1}{e} \sum_{k=0}^{\infty} \frac{[k]_n}{k!} .$$

Si $\varphi(x) = \sum_n \alpha_n [x]_n$, on a

$$L(\varphi(x)) = \sum_n \alpha_n \sum_k \frac{1}{e} \frac{[k]_n}{k!} = \frac{1}{e} \sum_k \frac{1}{k!} \sum_n \alpha_n [k]_n = \frac{1}{e} \sum_k \frac{\varphi(k)}{k!} .$$

En faisant $\varphi(x) = x^{n+1}$, on obtient la formule annoncée.

2

Problèmes de partages

§ 1. P_n^m ou le nombre de partages de l'entier n en m parts

Dans le chapitre 1, nous avons dénombré les partitions en classes d'un ensemble X ; nous nous proposons ici de dénombrer les différents *types* des partitions d'un ensemble de n objets. A chaque type correspond une suite $(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_m)$ avec

$$n = \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_m ,$$
$$\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3 \geqslant \cdots \geqslant \alpha_m \geqslant 1 .$$

Cette suite décroissante est plus communément appelée *partage de l'entier n.* On désignera par P_n^m le nombre de partages de l'entier n en exactement m parts.

Exemple

Les partages de	sont	D'où
2	2 et 1 + 1	$P_2^1 = P_2^2 = 1$
3	3 et 2 + 1 et 1 + 1 + 1	$P_3^1 = P_3^2 = P_3^3 = 1$
4	4 et 3 + 1 et 2 + 2	$P_4^2 = 2$
	et 2 + 1 + 1 et 1 + 1 + 1 + 1	$P_4^1 = P_4^3 = P_4^4 = 1$

Relations de récurrence

On a

$$\boxed{\begin{array}{c} P_n^1 + P_n^2 + \cdots + P_n^k = P_{n+k}^k \\ P_n^1 = P_n^n = 1 \end{array}} .$$

Seule la première formule est à démontrer ; soit E l'ensemble des partages de n ayant un nombre de parts $\leqslant k$; chaque partage de E peut être considéré comme un k-uple (dont les derniers coefficients, éventuellement, seraient nuls).

Définissons sur E l'application

$$(\alpha_1, \alpha_2, ..., \alpha_m, 0, 0, ..., 0) \to (\alpha_1 + 1, \alpha_2 + 1, ..., \alpha_m + 1, 1, 1, ..., 1) .$$

Elle applique E dans l'ensemble E' des partages de $n + k$ en exactement k parts. Cette application est bijective, car

1° Deux k-uples différents de E donnent deux k-uples différents de E'.

2° Tout k-uple de E' est l'image d'un k-uple de E. Donc

$$| E | = P_n^1 + \cdots + P_n^k = | E' | = P_{n+k}^k .$$

On obtient aussi des formules de récurrence pour calculer les P_n^m, ce qui donne :

P_n^m	$m=1$	2	3	4	5	6	...
$n=1$	1	0	0	0	0	0	
2	1	1	0	0	0	0	
3	1	1	1	0	0	0	
4	1	2	1	1	0	0	
5	1	2	2	1	1	0	
6	1	3	3	2	1	1	

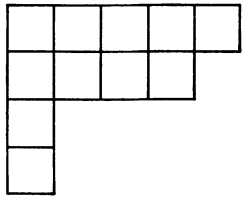
PROPOSITION 1. *Le nombre de partages de n ayant k pour plus grande part est égal au nombre P_n^k de partages de n en k parts.*

Par exemple, pour $n = 6$, on trouve trois partages ayant 3 pour plus grande

part : $3 + 1 + 1 + 1$, $3 + 2 + 1$, $3 + 3$; on trouve trois partages en 3 parts : $4 + 1 + 1$, $3 + 2 + 1$, $2 + 2 + 2$.

Pour démontrer cette propriété, considérons un partage, par exemple $5 + 4 + 1 + 1$, associons-lui un diagramme (appelé parfois *diagramme de Ferrers*) en représentant chaque part par une rangée de carrés en nombre égal à la part considérée, et disposés de la façon suivante :

$5 + 4 + 1 + 1 \quad \rightarrow$



On appelle *partage conjugué* du partage $\alpha = (\alpha_1, \alpha_2, ..., \alpha_k)$ le partage $\alpha^* = (\alpha_1^*, \alpha_2^*, ...)$, où α_i^* est le nombre de parts de α qui sont $\geqslant i$. Il lui correspond un diagramme de Ferrers symétrique du précédent par rapport à la diagonale.

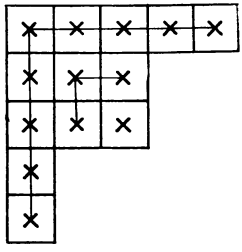
Le partage conjugué de $5 + 4 + 1 + 1$ est $4 + 2 + 2 + 2 + 1$, comme on le voit immédiatement sur le diagramme de Ferrers ci-dessus : on compte le nombre de carrés dans la première colonne, puis le nombre de carrés dans la deuxième colonne, etc.

L'application qui fait correspondre à chaque partage de n son conjugué est bijective ; on établit ainsi une correspondance bi-univoque entre les partages de n ayant k pour plus grande part et les partages de n en k parts.

PROPOSITION 2. *Les partages de n qui sont identiques à leurs conjugués sont aussi nombreux que les partages de n en parts toutes inégales et impaires.*

En effet, à tout partage en parts inégales et impaires, on peut faire correspondre un diagramme de Ferrers en écrivant chacune des parts en équerre, comme ci-dessous :

$9 + 3 + 1 \quad \rightarrow$



$\rightarrow \quad 5 + 3 + 3 + 1$

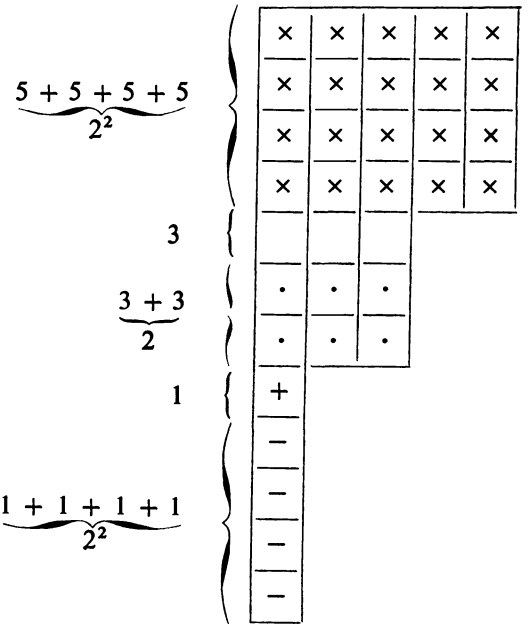
Ce diagramme de Ferrers définit un partage conjugué à lui-même (ici le partage $5 + 3 + 3 + 1 + 1$) ; la correspondance est bi-univoque.

PROPOSITION 3. *Les partages de n avec des parts toutes inégales sont aussi nombreux que les partages de n avec des parts toutes impaires.*

Considérons un partage avec des parts toutes impaires, soit par exemple $\underbrace{5+5+5+5}_{4}+\underbrace{3+3+3}_{3}+\underbrace{1+1+1+1+1}_{5}$: chaque exposant peut se décomposer d'une façon unique en somme de puissances de 2 (décomposition binaire), soit ici :

$$4 = 2^2$$
$$3 = 2^0 + 2$$
$$5 = 2^0 + 2^2.$$

On peut donc grouper 2^k parts identiques du diagramme de Ferrers comme sur la figure suivante :



Groupons les carrés inclus dans la même accolade.

On définit ainsi un nouveau partage, à savoir 20 + 6 + 4 + 3 + 1 dont toutes les parts sont inégales, puisque chaque nombre s'écrit d'une façon unique comme le produit d'un nombre impair et d'une puissance de 2.

Comme la correspondance est bi-univoque, on a bien démontré la proposition.

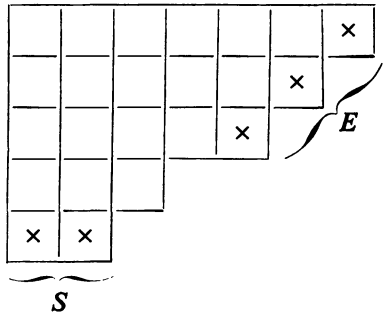
PROPOSITION 4. *Soit Q_n le nombre de partages de n avec un nombre pair de parts, et des parts toutes inégales ; soit Q'_n le nombre de partages de n avec un nombre impair de parts, et des parts toutes inégales. On a*

$$Q_n = \begin{cases} Q'_n & \text{si} \quad n \neq \frac{k}{2}(3k \pm 1) \\ Q'_n + (-1)^k & \text{si} \quad n = \frac{k}{2}(3k \pm 1) \end{cases}$$

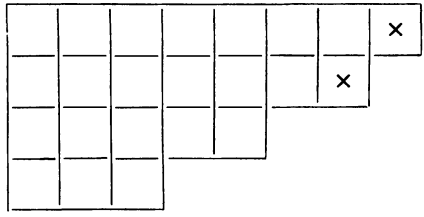
En effet, considérons un partage de n avec un nombre impair de parts, et des parts toutes inégales ; soit S l'ensemble des carrés de la ligne horizontale à l'extrême Sud de son diagramme de Ferrers ; soit E l'ensemble des carrés de la ligne à 45° à l'extrême Est (les deux lignes pouvant d'ailleurs se borner à un carré unique).

Par exemple,

$7 + 6 + 5 + 3 + 2 \quad \rightarrow$



Si $|S| \leqslant |E|$, je transporte la ligne S à l'extrême Est du diagramme de Ferrers, soit ici :

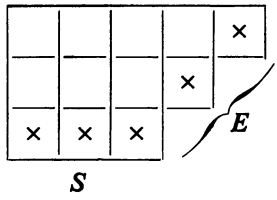


J'obtiens ainsi le nouveau partage $8 + 7 + 5 + 3$, avec un nombre pair de parts, et toutes inégales (et avec $|S| > |E|$). Si l'on avait eu initialement $|S| > |E|$, je porterais la ligne E à l'extrême Sud, pour obtenir un nouveau partage avec un nombre pair de parts et toutes inégales (et avec $|S| \leqslant |E|$).

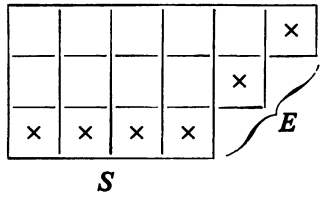
Cette transformation est toujours possible, excepté si les lignes S et E se rencontrent, avec en outre :

$$|S| = |E|, \quad \text{ou} \quad |S| = |E| + 1.$$

Cas $|S| = |E|$; on ne peut pas transporter S à l'Est.



Cas $|S| = |E| + 1$; on ne peut pas transporter E au Sud.



Si l'on pose $|E| = k$, $\varepsilon = 0$ ou 1, on a dans les cas d'exception :

$$n = (k+\varepsilon) + (k+\varepsilon+1) + (k+\varepsilon+2) + \cdots + (2k+\varepsilon-1) = \frac{k}{2}(3k+2\varepsilon-1)$$

$$= \frac{k}{2}(3k \pm 1).$$

Dans tous les autres cas, la correspondance est bijective ; d'où la formule annoncée.

C. Q. F. D.

Une autre façon d'étudier les nombres P_n^m est de recourir à la *méthode des fonctions génératrices*, due à Laplace et Euler.

Soit $\varphi(n)$ une fonction définie pour les entiers $n \geqslant 0$; on peut lui associer la fonction

$$F(x) = \sum_{n=0}^{\infty} \varphi(n)\, x^n$$

(en supposant que la série converge au voisinage de l'origine, ce qui sera toujours le cas ici). On dit alors que $F(x)$ est la *fonction génératrice* de $\varphi(n)$, ce que l'on écrira

$$\varphi(n) \doteqdot F(x).$$

On dit aussi que $\varphi(n)$ est l'*image* de la fonction $F(x)$, et l'on a :

$$\varphi(n) = \frac{1}{n!}\left[\frac{d^n F}{dx^n}\right]_0.$$

1° La fonction génératrice du nombre P_n des partages de l'entier n est :

$$F_1(x) = (1 - x)^{-1}(1 - x^2)^{-1}(1 - x^3)^{-1} \dots$$

(en posant arbitrairement $P_0 = 1$).

En effet, il s'agit de montrer qu'au voisinage de l'origine, on a

$$\frac{1}{(1 - x)(1 - x^2)(1 - x^3)\dots} = \sum_{n=0}^{\infty} P_n x^n .$$

En effet, on a, pour $|x| < 1$,

$$\frac{1}{(1 - a_1 x)(1 - a_2 x^2)\dots(1 - a_k x^k)\dots} = (1 + a_1 x + a_1^2 x^2 + a_1^3 x^3 + \cdots)$$
$$(1 + a_2 x^2 + a_2^2 x^4 + \cdots)\dots(1 + a_k x^k + a_k^2 x^{2k} + \cdots)\dots$$
$$= 1 + a_1 x + \cdots + (a_1^{\lambda_1} a_2^{\lambda_2} \dots a_k^{\lambda_k} + \cdots) x^n + \cdots$$

Dans le coefficient de x^n, chaque terme $a_1^{\lambda_1} a_2^{\lambda_2} \dots a_k^{\lambda_k}$ définit un partage de n, à savoir :

$$\underbrace{(1 + 1 + \cdots + 1)}_{\lambda_1} + \underbrace{(2 + 2 + \cdots + 2)}_{\lambda_2} + \cdots + \underbrace{(k + k + \cdots + k)}_{\lambda_k} = n .$$

On a ainsi tous les partages de n sans omissions ni répétitions. Donc, en faisant $1 = a_1 = a_2 = \cdots$, on obtient la formule annoncée.

2° La fonction génératrice de P_n^m est

$$F_2(x) = x^m(1 - x)(1 - x^2)\dots(1 - x^m) .$$

3° La fonction génératrice du nombre de partages de n en parts impaires est

$$F_3(x) = (1 + x + x^2 + \dots)(1 + x^3 + x^6 + \cdots)(1 + x^5 + x^{10} + \cdots)\dots$$
$$= (1 - x)^{-1}(1 - x^3)^{-1}(1 - x^5)^{-1} \dots$$

4° La fonction génératrice du nombre de partages de n en parts toutes inégales est

$$F_4(x) = (1 + x)(1 + x^2)(1 + x^3)\dots$$

5° La fonction génératrice du nombre de partages de n en un nombre impair de parts est

$$F_5(x) = \prod_{i=1}^{\infty} (1 - x^{2i+1})^{-1} .$$

6° La fonction génératrice du nombre de partages de n en parts toutes distinctes est

$$F_6(x) = \prod_{i=1}^{\infty} (1 + x^i).$$

7° La fonction génératrice du nombre de partages de n à parts impaires distinctes est

$$F_7(x) = \prod_{i=1}^{\infty} (1 + x^{2i+1}).$$

Application d'identités remarquables aux dénombrements de partages

Reprenons par exemple la proposition 3 : les partages de n avec des parts toutes inégales sont aussi nombreux que les partages de n en parts toutes impaires.

Il s'agit de montrer que

$$F_3(x) = \frac{1}{(1 - x)(1 - x^3)(1 - x^5)\ldots}$$

et

$$F_4(x) = (1 + x)(1 + x^2)(1 + x^3)\ldots$$

sont identiques.

On a en effet

$$F_3(x) = \frac{(1 - x^2)(1 - x^4)(1 - x^6)\ldots}{(1 - x)(1 - x^2)(1 - x^3)\ldots} =$$

$$= \frac{(1 - x)(1 + x)(1 - x^2)(1 + x^2)\ldots}{(1 - x)(1 - x^2)\ldots} = F_4(x).$$

Cette démonstration, due à Euler, est très générale et ne nécessite pas une intuition exceptionnelle ; par contre, elle n'indique pas explicitement, une correspondance bi-univoque entre deux classes de partages.

Application des dénombrements de partages à des identités remarquables

Prenons l'identité d'Euler

$$(1 - x)(1 - x^2)(1 - x^3)\ldots = 1 + \sum \varphi(n)\, x^n = 1 - x - x^2 + x^5 + \cdots$$

L'image de cette fonction génératrice est

$$\varphi(n) = \begin{cases} 0 & \text{si} \quad n \neq \dfrac{3k^2 \pm k}{2} \\ (-1)^k & \text{si} \quad n = \dfrac{3k^2 \pm k}{2}. \end{cases}$$

Soit Q_n le nombre de partages de n en parts toutes inégales, avec un nombre pair de parts ; soit Q'_n le nombre de partages de n en parts toutes inégales, avec un nombre impair de parts.

Le coefficient de x^n dans le produit considéré est égal à $Q_n - Q'_n$; ce nombre est égal à $\varphi(n)$, d'après la proposition 4.

C. Q. F. D.

Il existe d'autres identités de ce genre, dont les plus célèbres sont celles de JACOBI et de ROGERS-RAMANUJAN ; le fait le plus remarquable est qu'elles s'expriment toutes en termes de partages. En outre, elles permettent d'étudier le comportement asymptotique des nombres P_n, P_n^m.

C'est ainsi que HARDY et RAMANUJAN donnent :

$$\operatorname{Log} P_n \sim \pi \sqrt{\frac{2n}{3}} - \operatorname{Log}(4n\sqrt{3}).$$

(Cf. WRIGHT, [12]).

§ 2. *$P_{n,h}$, ou le nombre de partages de l'entier n dont la plus petite part est h*

Nous désignons ici par :

- P_n le nombre de partages de n,
- P_n^m le nombre de partages de n en m parts,
- $P_{n,h}$ le nombre de partages de n dont la plus petite part est h,
- $P_{n,h}^m$ le nombre de partages de n en m parts dont la plus petite part est h.

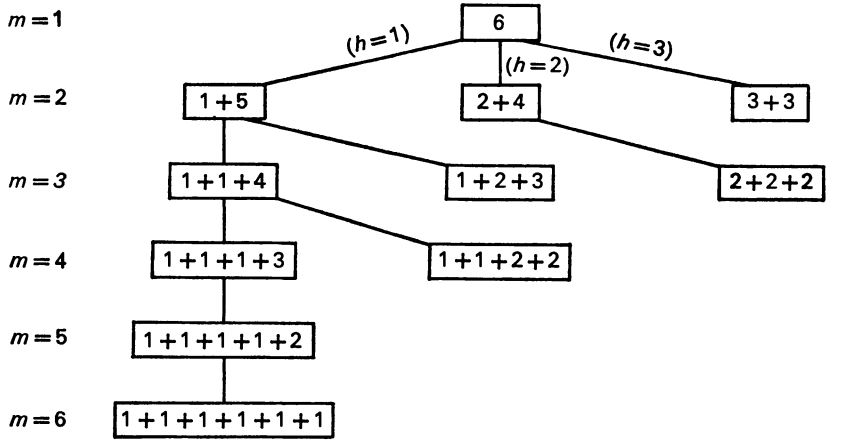
On a les formules évidentes :

$$P_n = P_n^1 + P_n^2 + \cdots + P_n^n,$$

$$P_n^m = P_{n,1}^m + P_{n,2}^m + \cdots + P_{n,n}^m,$$

$$P_{n,h} = P_{n,h}^1 + P_{n,h}^2 + \cdots + P_{n,h}^n.$$

Exemple. Considérons les partages de 6 en m parts, avec une plus petite part égale à h. Ces partages peuvent se représenter par un arbre de la façon suivante :



Cette représentation est commode quand on veut retrouver rapidement un nombre $P^m_{n,h}$. On voit immédiatement, en descendant l'arbre : $P^4_{6,1} = 2$, etc. (P. BERTIER [2]).

Formule 1

$$\boxed{\begin{array}{lll} P^m_{n,h} = P^m_{n-m,h-1} & \text{si} & h > 1 \\ P^m_{n,h} = P^{m-1}_{n-1} & \text{si} & h = 1 \end{array}}\,.$$

Supposons $h > 1$; à tout partage $n = \alpha_1 + \alpha_2 + \cdots \alpha_m$, avec

$$\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_m = h\,,$$

on peut associer le partage :

$$n - m = (\alpha_1 - 1) + (\alpha_2 - 1) + \cdots + (\alpha_{m-1} - 1) + (h - 1)\,.$$

Formule 2

$$\boxed{P_{n,h} = P_{n-h,h} + P_{n-h,h+1} + \cdots}\,.$$

En effet, on peut écrire

$$n = h + (n - h)\,.$$

Donc

$$P_{n,h} = \sum_{k \geqslant h} P_{n-h,k} .$$

Relations de récurrence

$$\boxed{\begin{array}{lll} P_{n,h} = P_{n-1,h-1} - P_{n-h,h-1} & \text{si} & h > 1 \\ P_{n,h} = P_{n-1} & \text{si} & h = 1 \end{array}} .$$

Supposons $h > 1$; d'après la formule 2, on a :

$$P_{n-1,h-1} = \sum_{k \geqslant h-1} P_{n-h,k} .$$

D'où, en comparant avec la formule 2,

$$P_{n,h} = P_{n-1,h-1} - P_{n-h,h-1} .$$

Cette dernière formule permet de construire le tableau suivant, colonne par colonne :

$P_{n,h}$	$h = 1$	$h = 2$	$h = 3$	$h = 4$	$h = 5$ ...	P_n
$n = 1$	1	0	0	0	0 ...	1
$n = 2$	1	1	0	0	0 ...	2
$n = 3$	2	0	1	0	0 ...	3
$n = 4$	3	1	0	1	0 ...	5
$n = 5$	5	1	0	0	1 ...	7
$n = 6$	7	2	1	0	0 1 ...	11
$n = 7$	11	2	1	0	0 ... 1 ...	15
$n = 8$	15	4	1	1	0 ... 1 ...	22
$n = 9$	22	4	2	1	0 ... 1 ...	30
$n = 10$	30	7	2	1	1 ... 1 ...	42
...						

§ 3. *Dénombrement des tableaux standards associés à un partage de n*

Etant donné un partage $\alpha_1 + \alpha_2 + \cdots + \alpha_m = n$ (avec $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_m$), on appelle *tableau associé à ce partage* une matrice $((k^i_j))$ d'entiers telle que la i-ième ligne de la matrice $(k^i_1, k^i_2, \ldots, k^i_{\alpha i})$ contient exactement α_i entiers.

Le tableau est dit *normal* si :

(1) les k_j^i sont tous distincts,

(2) $i > j \Rightarrow k_s^i > k_s^j$,

(3) $i > j \Rightarrow k_i^t > k_j^t$.

Par exemple, la matrice

$$((k_j^i)) = \begin{array}{|c|c|c|} \hline 1 & 3 & 6 \\ \hline 2 & 4 \\ \cline{1-2} 5 & 7 \\ \cline{1-2} \end{array}$$

est un tableau normal associé au partage 3 + 2 + 2 : en effet, les entiers vont en croissant quand on lit une ligne de gauche à droite, ou quand on lit une colonne de haut en bas.

Un tableau normal associé à un partage de n et rempli avec les entiers 1, 2, ..., n, est appelé un *tableau standard.* Le but que nous nous proposons ici est de dénombrer les tableaux standards associés à un partage donné ; ce problème a en effet de nombreuses applications en analyse (1).

Exemples. Le nombre de tableaux standards associés au partage 3 + 2 + 2 est 21 ; la liste est la suivante :

...	123	124	134	125	135	
..	45	35	25	34	24	
67	67	67	67	67	67	
...	123	124	134	125	135	145
. 6	46	36	26	36	26	26
. 7	57	57	57	47	47	37
.. 6	126	136	126	136	146	
..	34	24	35	25	25	
. 7	57	57	47	47	37	
.. 7	127	137	127	137	147	
..	34	24	35	25	25	
. 6	56	56	46	46	36	

On remarque que l'entier le plus élevé du tableau (ici 7) doit apparaître nécessairement à l'extrémité droite d'une rangée et en bas d'une colonne

(1) Cf. à ce sujet : D. E. RUTHERFORD [9].

(soit, ici, deux places possibles). On les essaiera toutes successivement en partant de la dernière rangée.

Si on élimine la case du chiffre 7, on place le chiffre 6 successivement dans toutes les cases (i, j) qui se trouvent à l'extrémité droite d'une rangée et en bas d'une colonne dans le nouveau diagramme (soit ici trois places possibles) ; etc...

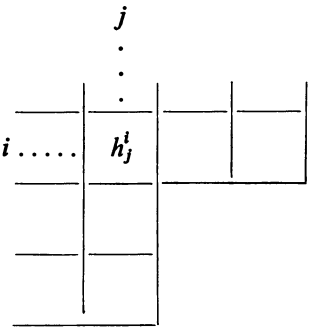
Etant donné un partage

$$\alpha_1 + \alpha_2 + \cdots + \alpha_m = n, \qquad \alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_m \geqslant 1 ,$$

on appelle *tableau des équerres* la matrice des nombres :

$$h_j^i = 1 + (\alpha_i - j) + (\alpha_j^* - i) .$$

On obtient ce tableau en représentant le partage par un diagramme de Ferrers



A la case (i, j), intersection de la i-ième ligne et de la j-ième colonne, on dénombre : la case (i, j), puis les cases à sa droite (en nombre $\alpha_i - j$), puis les cases en dessous d'elle (en nombre $\alpha_j^* - i$). Ainsi le tableau d'équerre correspondant au partage $3 + 2 + 2$ est

$$((h_j^i)) = \begin{array}{|c|c|c|} \hline 5 & 4 & 1 \\ \hline 3 & 2 & \multicolumn{1}{c}{} \\ \cline{1-2} 2 & 1 & \multicolumn{1}{c}{} \\ \cline{1-2} \end{array}$$

LEMME. *Pour une case (i, j) donnée, la suite*

$$(h_j^i, h_{j+1}^i, \ldots, h_{\alpha_i}^i, h_j^i - h_j^{i+1}, h_j^i - h_j^{i+2}, \ldots, h_j^i - h_j^{\alpha_j^*})$$

constitue une permutation des entiers $1, 2, \ldots, h_j^i$.

Considérons l'équerre ayant pour angle la case (i, j), soit :

i, j	$i, j+1$	$i, j+2$	...	$i, j+p$
$i+1, j$				
$i+2, j$				
. . .				
$i+q, j$				

Cet équerre contient h_j^i cases.

Mettons dans la case

(i, j) le nombre h_j^i

$(i, j+1)$ le nombre h_{j+1}^i

.....

$(i+1, j)$ le nombre $h_j^i - h_j^{i+1}$, etc.

.....

Montrons qu'on n'a pas inscrit deux fois le même nombre ; la suite inscrite dans la première rangée de l'équerre est évidemment strictement décroissante ; la suite inscrite sous (i, j) est strictement croissante, avec le dernier terme :

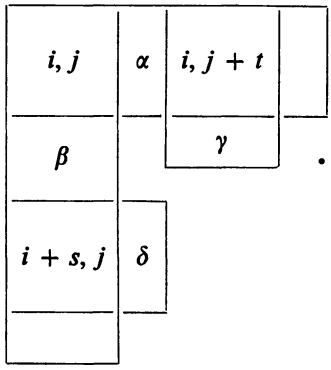
$$h_j^i - h_j^{\alpha_j^*} < h_j^i .$$

Il suffit donc de montrer que pour $t \geqslant 1$, $s \geqslant 1$, on ne peut pas avoir

$$h_{j+t}^i = h_j^i - h_j^{i+s} .$$

Pour cela, considérons les trois équerres ayant respectivement pour angles les cases (i, j), $(i, j + t)$ et $(i + s, j)$; désignons par :

α le nombre de cases entre (i, j) et $(i, j + t)$,
β le nombre de cases entre (i, j) et $(i + s, j)$,
γ le nombre de cases en dessous de $(i, j + t)$,
δ le nombre de cases à droite de $(i + s, j)$.



L'égalité précédente s'écrit :

$$h^i_{j+t} + h^{i+s}_j = h^i_j ,$$

ou :

$$\gamma + \delta = \alpha + \beta + 1 .$$

Si l'on a $\delta \leqslant \alpha$, $\gamma \leqslant \beta$, cette égalité devient $\gamma + \delta \geqslant \gamma + \delta + 1$: absurde. Si l'on a $\delta > \alpha$, cela implique que les équerres d'angles $(i + s, j)$ et $(i, j + t)$ intersectent, donc $\gamma > \beta$, et l'égalité devient

$$\gamma + \delta = \alpha + \beta + 1 \leqslant (\delta - 1) + (\gamma - 1) + 1 = \gamma + \delta - 1 : \text{absurde.}$$

C. Q. F. D.

THÉORÈME DE FRAME-ROBINSON-THRALL. *Etant donné un partage*

$$\alpha_1 + \alpha_2 + \cdots + \alpha_m = n$$

de l'entier n, soit $((h^i_j))$ *le tableau d'équerre qui lui correspond. Le nombre de tableaux standards associés au partage donné est* :

$$f(\alpha_1, \ldots, \alpha_m) = \frac{n!}{\prod_{i,j} h^i_j} .$$

En vertu du lemme, on a

$$\prod_{i,j} h^i_j = \prod_{i=1}^{m} \prod_{j=1}^{\alpha_1} h^i_j = \frac{\prod_{i \geqslant 1} (h^i_1)!}{\prod_{\substack{i \geqslant 1 \\ j > i}} (h^i_1 - h^j_1)} .$$

Posons :

$$x_i = h^i_1 = \alpha_i + (m - i) .$$

La fonction f définie par l'énoncé peut alors s'écrire :

$$f(\alpha_1, \alpha_2, \ldots, \alpha_m) = n! \frac{\prod_{\substack{i \geqslant 1 \\ j > i}} (x_i - x_j)}{\prod_{i \geqslant 1} (x_i)!}.$$

On a aussi :

$$f(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_m)$$

$$= (n-1)! \frac{\prod_{\substack{i,j \neq k \\ j > i}} (x_i - x_j) \prod_{j > k} (x_k - 1 - x_j) \prod_{i < k} (x_i - x_k + 1)}{\prod_{i \neq k} (x_i)! \, (x_k - 1)!}$$

$$= \frac{x_k}{n} f(\alpha_1, \alpha_2, \ldots, \alpha_m) \prod_{j \neq k} \frac{(x_k - 1 - x_j)}{(x_k - x_j)}.$$

Remarquons que si $\alpha_{k+1} = \alpha_k$, on a $x_{k+1} = x_k - 1$, et cette expression est nulle.

Raisonnons par induction : la formule de l'énoncé est vraie pour des partages de $n = 1, 2$; supposons la vraie pour les partages d'entiers inférieurs à n, et démontrons-la pour le partage $\alpha_1 + \alpha_2 + \cdots + \alpha_m = n$.

Dans un tableau standard T_n d'ordre n, associé au partage $\alpha_1, \alpha_2, \ldots, \alpha_m$, le chiffre n se trouve à l'extrémité d'une ligne k pour laquelle $\alpha_{k+1} < \alpha_k$. La suppression du chiffre n fait correspondre à T_n un tableau standard T_{n-1}, associé au partage $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_m$, et on établit ainsi une bijection entre l'ensemble de tous les tableaux standards T_n et un ensemble de tableaux standards d'ordre $n - 1$. Le nombre de tableaux standards d'ordre n est donc

$$\sum_{k / \alpha_{k+1} \neq \alpha_k} f(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_m)$$

$$= \sum_{k=1}^{m} f(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_m)$$

$$= \frac{1}{n} f(\alpha_1, \ldots, \alpha_m) \sum_{k=1}^{m} x_k \prod_{j \neq k} \frac{(x_k - x_j - 1)}{(x_k - x_j)}.$$

Posons

$$g(x) = \prod_{j=1}^{m} (x - x_j).$$

Il s'agit donc de montrer que si les m racines d'un polynôme $g(x)$ vérifient

$$x_1 < x_2 < \cdots < x_m$$

$$\sum_{i=1}^{m} x_i = \sum_{i=1}^{m} \alpha_i + \sum_{i=1}^{m} (m - i) = n + \frac{m(m-1)}{2},$$

elles vérifient également :

$$n = \sum_{k=1}^{m} x_k \prod_{j \neq k} \frac{(x_k - x_j - 1)}{(x_k - x_j)} = \sum_{k=1}^{m} \frac{(-x_k)\, g(x_k - 1)}{g'(x_k)}$$

(Cette vérification, qui sera laissée au lecteur, est une routine habituelle dans la théorie des fonctions symétriques des racines d'un polynôme.)

G. de B. ROBINSON ([8]) a découvert (1) une construction remarquable qui associe de façon injective à une suite φ formée d'entiers différents, une paire $P(\varphi)$, $Q(\varphi)$ de tableaux standards de mêmes formes. Nous allons donner maintenant cette construction, qui a été présentée indépendamment par C. SCHENSTED [10] dont nous conservons la terminologie et les notations.

Soit T un tableau normal, formé d'entiers distincts $k_1, k_2, \ldots, k_n$. Si

$$x \neq k_1, k_2, \ldots, k_n,$$

on peut former un nouveau tableau au moyen des règles suivantes :

1° On place x dans la première rangée, soit en remplaçant par x le plus petit k_i qui est $> x$, soit si un tel k_i n'existe pas en ajoutant x à la fin de cette première rangée ;

2° si x a remplacé le symbole k_i de la première rangée, on place k_i dans la deuxième rangée suivant la même loi, etc.

Un tel tableau sera désigné par $(T \leftarrow x)$.

Exemple. Si

$$(T) = \begin{array}{ll} 2 & 4\ 7 \\ 3 & 8 \\ 5 & 9 \end{array}$$

on a :

$$(T \leftarrow 6) = \begin{array}{lll} 2 & 4 & 6 \\ 3 & 7 & \\ 5 & 8 & \\ 9 & & \end{array}$$

On remarque immédiatement que $(T \leftarrow x)$ *est aussi un tableau normal.*

---

(1) Nous devons cette référence à l'obligeance de M. P. SCHÜTZENBERGER.

Pour une suite φ d'entiers distincts $k_1, k_2, \ldots, k_n$, on désigne par $P(\varphi)$ le tableau standard :

$$[((k_1) \leftarrow k_2) \leftarrow k_3] \leftarrow k_4 \ldots$$

On désigne par $Q(\varphi)$ le tableau de même diagramme en plaçant l'entier i dans la case ajoutée au diagramme au moment où l'on a incorporé l'entier k_i.

Exemple. Prenons la suite 3, 5, 4, 9, 8. On forme successivement :

$\varphi =$	3	3 5	3 5 4	3 5 4 9	3 5 4 9 8
$P(\varphi) =$	3	3 5	3 4 5	3 4 9 5	3 4 8 5 9
$Q(\varphi) =$	1	1 2	1 2 3	1 2 4 3	1 2 4 3 5

Inversement, si l'on se donne $P(\varphi) = \begin{matrix} 3 & 4 & 8 \\ 5 & 9 \end{matrix}$ et $Q(\varphi) = \begin{matrix} 1 & 2 & 4 \\ 3 & 5 \end{matrix}$, on peut aisément retrouver la suite φ initiale en procédant de façon inverse : le dernier entier déplacé dans le tableau P est le 9, qui ne peut provenir de la première ligne que lorsqu'on a incorporé le 8 : donc le dernier entier de la suite est 8 ; etc.

On remarque que $Q(\varphi)$ *est un tableau standard* ; en effet, $P(\varphi)$ est un tableau normal d'après la remarque précédente, et $Q(\varphi)$ a le même diagramme ; comme chaque entier ajouté au tableau $Q(\varphi)$ est plus grand que ceux qui sont au-dessus ou à sa gauche (qui ont été placés avant), $Q(\varphi)$ est aussi un tableau normal ; c'est donc un tableau standard. On peut d'ailleurs remarquer (M. P. SCHÜTZENBERGER [11]) que pour une permutation φ, on a $Q(\varphi) = P(\varphi^{-1})$.

LEMME (ROBINSON). *Le nombre de colonnes de $P(\varphi)$ est égal à la longueur de la plus grande suite partielle croissante de la suite φ ; le nombre de rangées de $P(\varphi)$ est égal à la longueur de la plus longue suite partielle décroissante de la suite φ.*

1° On appelle j-ième *suite fondamentale* d'une suite φ celle fournie par les différents entiers placés à la j-ième place de la première rangée des tableaux P ; *chaque suite fondamentale est une suite partielle décroissante de la suite initiale* (immédiat).

Dans l'exemple précédent, les suites fondamentales sont : 3 ; 5, 4 ; 9, 8.

2° Etant donné un entier k de la j-ième suite fondamentale, *on peut trouver un entier de la $(j-1)$-ième suite fondamentale qui est plus petit et qui apparaît à gauche dans la séquence donnée φ.*

L'entier qui occupe la $(j-1)$-ième place de la première rangée lorsque l'élé-

ment k est incorporé au tableau P à la j-ième place, répond aux conditions proposées.

3° Le nombre de colonnes de $P(\varphi)$ est le même que celui des suites fondamentales ; d'après (1), il ne peut exister plus d'un élément de chaque suite fondamentale dans une suite partielle croissante de φ ; d'après (2), on peut construire une suite partielle croissante de φ avec un élément pris dans chaque suite fondamentale. Donc : *le nombre de colonnes de $P(\varphi)$ est la longueur de la plus longue suite partielle croissante de φ.*

4° La seconde partie de l'énoncé découle du fait qu'en écrivant une suite à l'envers, on change les suites croissantes en suites décroissantes.

Remarquons que ce raisonnement permet facilement d'obtenir des suites partielles croissantes de longueur maximale, à savoir, pour l'exemple ci-dessous :

$$3, 4, 8 \qquad \text{et} \qquad 3, 4, 9 .$$

THÉORÈME DE SCHENSTED. *Le nombre de permutations de* 1, 2, ..., n *dont la plus longue suite partielle croissante est de longueur p et la plus longue suite partielle décroissante est de longueur q, est obtenu en comptant les tableaux standards associés aux différents partages de n avec q parts et de plus grande part égale à p, et en sommant les carrés des nombres obtenus.*

En effet, à chaque permutation φ satisfaisant aux conditions proposées correspondent un $P(\varphi)$ et un $Q(\varphi)$, qui sont deux tableaux standards de mêmes formes avec p colonnes et q rangées ; inversement, à tout couple de tableaux standards de mêmes formes, avec p colonnes et q rangées, il correspond une permutation satisfaisant aux conditions proposées (et une seule). D'où le résultat annoncé.

Exemple. Pour $n = 10$, $p = 6$, $q = 3$, on considère les tableaux d'équerre :

8	6	5	3	2	1
4	2	1			
1					

8	7	4	3	2	1
3	2				
2	1				

D'après le théorème de SCHENSTED, le nombre de permutations cherchées est :

$$\left(\frac{10!}{2.3.5.6.8.4.2}\right)^2 + \left(\frac{10!}{2.3.4.7.8.2.3.2}\right)^2 = (315)^2 + (225)^2 = 149.850$$

§ 4. *Une application du treillis de Young*

Considérons deux suites $\alpha = (\alpha_1, \alpha_2, ..., \alpha_p, 0, 0, ...)$ et

$$\beta = (\beta_1, \beta_2, ..., \beta_q, 0, 0, ...),$$

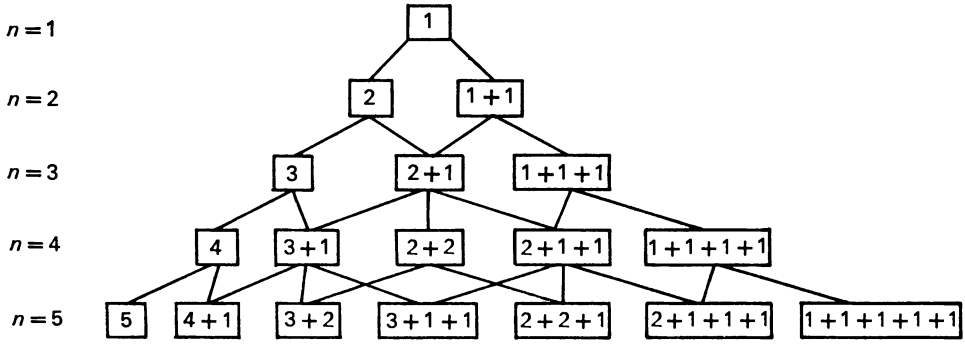
avec

$$\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3 \geqslant \cdots \geqslant \alpha_p,$$
$$\beta_1 \geqslant \beta_2 \geqslant \beta_3 \geqslant \cdots \geqslant \beta_q.$$

Elles correspondent à des partages de deux entiers $\sum_i \alpha_i$ et $\sum_j \beta_j$ non nécessairement égaux. Posons

$$\alpha \vee \beta = (\max\{\alpha_1, \beta_1\}, \max\{\alpha_2, \beta_2\}, ...),$$
$$\alpha \wedge \beta = (\min\{\alpha_1, \beta_1\}, \min\{\alpha_2, \beta_2\}, ...).$$

Ce sont encore des suites décroissantes se terminant par des 0. Ces opérations définissent un treillis, appelé treillis de YOUNG, qui commence ainsi :
niveaux :



Le nombre de sommets du niveau n est P_n ; si un partage contient k entiers *distincts*, il admet k prédécesseurs et $k + 1$ successeurs.

La propriété fondamentale des treillis de Young est la suivante :

THÉORÈME DE KREWERAS ([5]). *Soient* $\alpha = (\alpha_1, \alpha_2, ..., \alpha_m, 0, 0, ...)$ *et* $\beta = (\beta_1, \beta_2, ..., \beta_n, 0, 0, ...)$ *deux suites de Young avec* $\beta \leqslant \alpha$, *c'est-à-dire* $\beta_i \leqslant \alpha_i$, *et appelons r-chaîne entre* β *et* α *une séquence* $\beta, \gamma^1, \gamma^2, ..., \gamma^r, \alpha$, *avec* :

$$\beta < \gamma^1 < \gamma^2 < \cdots < \gamma^r < \alpha.$$

Le nombre $w_r(\beta, \alpha)$ *de r-chaînes entre* β *et* α *est égal au déterminant d'ordre* $\max\{m, n\}$, *dont l'élément général (ligne i et colonne j) est* :

$$\binom{\alpha_i - \beta_j + r}{i - j + r}.$$

Pour deux entiers p et n pas nécessairement $\geqslant 0$, on pose ici :

$$\binom{n}{p} = \begin{cases} \dfrac{n(n-1)(n-2)\ldots(p+1)}{(n-p)!} & \text{si} \quad n > p \\ 1 & \text{si} \quad n = p \\ 0 & \text{si} \quad n < p \end{cases}$$

Pour la démonstration qui se fait par induction sur $\max\{m, n\}$, nous renvoyons le lecteur à KREWERAS [5].

Ce théorème permet en particulier de donner sous forme de déterminant :

1° Le nombre de partages γ avec $\beta < \gamma < \alpha$ (cas $r = 1$).

2° Le nombre de chemins dans le treillis de Young entre β et α $\left(\text{cas } r = \sum_i \alpha_i - \sum_j \beta_j - 1\right)$.

COROLLAIRE (KREWERAS [5]). *Le nombre de tableaux standards d'ordre n ayant pour diagramme le diagramme de Ferrers associé à un partage $\alpha = (\alpha_1, \alpha_2, \ldots)$ de n, et dans lesquels les entiers $1, 2, \ldots, p$ (avec $p < n$) remplissent le diagramme de Ferrers associé à un partage $\beta = (\beta_1, \beta_2, \ldots)$ de p, est égal au nombre de chemins entre β et α dans le treillis de Young* (qui est déterminé par le théorème précédent).

On se propose de calculer le nombre de tableaux standards T d'ordre n ayant un diagramme donné et dans lesquels les entiers $1, 2, \ldots, p$ $(p < n)$ ont des places fixées à l'avance, qui constituent un tableau standard S d'ordre p. On obtiendra le tableau standard T à partir de S en ajoutant successivement les entiers $p+1, p+2, \ldots, n$, ce qui détermine une suite de partages ; soit par exemple :

$$S = \begin{matrix} 1\,2 \\ 3 \end{matrix} \rightarrow \begin{matrix} 1\,2\,4 \\ 3 \end{matrix} \rightarrow \begin{matrix} 1\,2\,4 \\ 3\,5 \end{matrix} \rightarrow T = \begin{matrix} 1\,2\,4 \\ 3\,5 \\ 6 \end{matrix}$$

Ceci détermine dans le treillis de Young le chemin :

$$\beta = (2, 1, 0, 0, \ldots) < (3, 1, \ldots) < (3, 2, \ldots) < \alpha = (3, 2, 1, \ldots).$$

Il y a ainsi une correspondance bi-univoque entre les tableaux standards T répondant aux conditions proposées et les chemins entre les partages α et β.

C. Q. F. D.

3

Formules d'inversion et applications

§ 1. *Opérateur de dérivation associé à une famille de polynômes*

Considérons une famille de polynômes d'une variable réelle x :

$$P_0(x)\ ,\ P_1(x)\ ,\ P_2(x)\ ,\ \ldots\ ;$$

Nous supposerons que $P_0(x) = 1$, et que pour $n \geqslant 1$, $P_n(x)$ est un polynôme de degré n en x qui s'annule pour $x = 0$. On dira alors qu'on a une *famille normale* de polynômes.

Un opérateur de dérivation associé aux polynômes $P_n(x)$ est une loi D qui fait correspondre à tout polynôme $\varphi(x)$ un polynôme que l'on note $D\varphi(x)$, avec en outre les propriétés suivantes :

(1°) $DP_n(x) = \begin{cases} nP_{n-1}(x) & \text{si } n \neq 0\ , \\ 0 & \text{si } n = 0\ ; \end{cases}$

(2°) $D[\lambda\varphi(x)] = \lambda\, D\varphi(x), \quad \lambda = \text{constante.}$

(3°) $D[\varphi(x) + \varphi'(x)] = D\varphi(x) + D\varphi'(x).$

PROPRIÉTÉ 1. *Pour toute famille normale de polynômes* P_n, *il existe un opérateur de dérivation* D *et un seul.*

En effet, tout polynôme $\varphi_n(x)$ de degré n peut s'écrire

$$\varphi_n(x) = \alpha_n\, P_n(x) + \alpha_{n-1}\, P_{n-1}(x) + \cdots + \alpha_0\, P_0(x)\ ,$$

où α_n, α_{n-1}, ..., α_0 sont des constantes, et cela d'une façon unique. En effet, il suffit de prendre pour α_n le coefficient de x^n dans $\varphi_n(x)$, divisé par le coeffi-

cient de x^n dans $P_n(x)$; $\varphi_{n-1}(x) = \varphi_n(x) - \alpha_0 P_n(x)$ est alors de degré $n-1$ (au plus) et l'on prendra pour α_{n-1} le coefficient de x^{n-1} dans $\varphi_{n-1}(x)$ divisé par le coefficient de x^{n-1} dans $P_{n-1}(x)$. On considère alors

$$\varphi_{n-2}(x) = \varphi_{n-1}(x) - \alpha_{n-1} P_{n-1}(x),$$

ce qui détermine α_{n-2}, etc.

En vertu de (1), (2), (3), on a :

$$D\varphi_n(x) = n\alpha_n P_{n-1}(x) + (n-1)\alpha_{n-1} P_{n-2}(x) + \cdots + 0.$$

Ceci prouve l'unicité de l'opérateur de dérivation associé aux polynômes $P_n(x)$.

En outre, l'opérateur D défini par cette égalité vérifie bien (1), (2), (3).

THÉORÈME DE TAYLOR RELATIF A UNE FAMILLE NORMALE DE POLYNÔMES $P_n(x)$. *Si φ est un polynôme de degré n en x, on a* :

$$\varphi(x) = \varphi(0) + \frac{D\varphi(0)}{1!} P_1(x) + \frac{D^2\varphi(0)}{2!} P_2(x) + \cdots + \frac{D^n\varphi(0)}{n!} P_n(x).$$

En outre, ce développement en série est unique.

On a

$$\varphi(x) = \alpha_0 P_0(x) + \alpha_1 P_1(x) + \cdots + \alpha_n P_n(x).$$

Si l'on fait $x = 0$, il vient

$$\varphi(0) = \alpha_0.$$

Dérivons :

$$D\varphi(x) = 0 + \alpha_1 P_0(x) + 2\alpha_2 P_1(x) + \cdots + n\alpha_n P_{n-1}(x).$$

Si l'on fait $x = 0$ dans le premier membre, on obtient

$$D\varphi(0) = \alpha_1.$$

Dérivons encore :

$$D^2\varphi(x) = 2\alpha_2 P_0(x) + 2\cdot 3\,\alpha_3 P_4(x) + \cdots + n(n-1)\alpha_n P_{n-2}(x).$$

D'où

$$D^2\varphi(0) = 2\alpha_2.$$

Plus généralement, si l'on pose

$$1 \times 2 \times 3 \times \cdots \times k = k!,$$

on trouve

$$D^k\varphi(0) = k!\,\alpha_k.$$

D'où la formule annoncée.

Remarquons que le polynôme $P_n(x) = x^n$ a pour opérateur de dérivation associé la dérivation ordinaire $\frac{d}{dx}$; on retrouve ainsi la formule classique de Taylor-MacLaurin.

Formule du binôme

Soit y une constante, et considérons le polynôme :

$$\varphi(x) = (x + y)^n .$$

Nous allons le développer en série de Taylor par rapport aux polynômes $P_n(x) = x^n$ (qui s'annulent bien pour $x = 0$, $n \neq 0$).

L'opérateur de dérivation associé aux polynômes P_n est la dérivation ordinaire

$$D\varphi(x) = \frac{d\varphi}{dx} .$$

On a

$$\begin{aligned} D\varphi(x) &= n(x + y)^{n-1} , \\ D^2\varphi(x) &= n(n - 1)(x + y)^{n-2} , \\ D^k\varphi(x) &= n(n - 1) \dots (n - k + 1)(x + y)^{n-k} . \end{aligned}$$

La formule de Taylor devient :

$$(x + y)^n = y^n + \binom{n}{1} xy^{n-1} + \binom{n}{2} x^2 y^{n-2} + \cdots + \binom{n}{n} x_n .$$

On retrouve la « formule du binôme », que l'on écrit aussi :

$$\boxed{(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}} .$$

Formule du binôme en Δ

Nous allons faire un développement en série par rapport aux polynômes :

$$P_n(x) = [x]_n = x(x - 1)(x - 2) \dots (x - n + 1) ;$$

ils s'annulent bien pour $x = 0$, $n \neq 0$.

Considérons l'opérateur Δ défini par

$$\Delta\varphi(x) = \varphi(x + 1) - \varphi(x) .$$

Δ est l'opérateur de dérivation associé aux polynômes P_n, car

$$\Delta[x]_n = [x + 1]_n - [x]_n = (x + 1)[x]_{n-1} - (x - n + 1)[x]_{n-1} = n[x]_{n-1} .$$

Suivant la formule de Taylor pour les polynômes $[x]_n$, développons le polynôme

$$\varphi(x) = [x + y]_n .$$

On a

$$\Delta^k \varphi(x) = n(n-1) \dots (n-k+1) [x+y]_{n-k} .$$

D'où finalement :

$$\boxed{[x + y]_n = \sum_{k=0}^{n} \binom{n}{k} [x]_k [y]_{n-k}} \quad \text{(Formule de Vandermonde)} .$$

Formule du binôme en ∇

Nous allons développer en série relativement aux polynômes :

$$P_n(x) = [x]^n = x(x+1)(x+2) \dots (x+n-1)$$

ils s'annulent bien pour $x = 0$, $n \neq 0$.

Considérons l'opérateur ∇ défini par

$$\nabla \varphi(x) = \varphi(x) - \varphi(x-1) .$$

C'est l'opérateur de dérivation associé aux polynômes P_n, car

$$\nabla [x]^n = [x]^n - [x-1]^n = (x+n-1)[x]^{n-1} - (x-1)[x]^{n-1} = n[x]^{n-1} .$$

Développons le polynôme

$$\varphi(x) = [x + y]^n ,$$

on a

$$\nabla^k \varphi(x) = n(n-1) \dots (n-k+1) [x+y]^{n-k} .$$

D'où

$$\boxed{[x + y]^n = \sum_{k=0}^{n} \binom{n}{k} [x]^k [y]^{n-k}} \qquad \text{(Formule de Nörlund).}$$

PREMIER THÉORÈME D'INVERSION. *Soient $\varphi_n(x)$ et $\psi_n(x)$ des polynômes de degré n avec les développements* :

$$\varphi_n(x) = \sum_{k=0}^{n} \alpha_n^k \psi_k(x) \qquad (n = 0, 1, 2, \dots, n_0)$$

$$\psi_n(x) = \sum_{k=0}^{n} \beta_n^k \varphi_k(x) \qquad (n = 0, 1, 2, \dots, n_0)$$

quels que soient les nombres $a_0, a_1, a_2, \ldots, a_{n_0}, b_0, b_1, b_2, \ldots, b_{n_0}$ *les relations*

$$a_n = \sum_{k=0}^{n} \alpha_n^k b_k \qquad (n = 0, 1, 2, \ldots, n_0)$$

impliquent :

$$b_n = \sum_{k=0}^{n} \beta_n^k a_k \qquad (n = 0, 1, 2, \ldots, n_0) .$$

En effet, on peut écrire

$$\varphi_n(x) = \sum_{k=0}^{n} \alpha_n^k \sum_{m=0}^{n} \beta_k^m \varphi_m(x) = \sum_{m=0}^{n} \left(\sum_{k=0}^{n} \alpha_n^k \beta_k^m \right) \varphi_m(x) .$$

On pose pour simplifier $\alpha_n^m = 0$ si $m > n$; $\beta_n^m = 0$ si $m > n$; $\delta_n^m = 0$ si $m \neq n$, $= 1$ si $m = n$; en identifiant les coefficients de $\varphi_m(x)$ dans les deux membres, on obtient :

$$\delta_n^m = \sum_{k=0}^{n_0} \alpha_n^k \beta_k^m .$$

Ceci exprime que les matrices $((\alpha_j^i))$ et $((\beta_j^i))$ sont inverses l'une de l'autre ; donc la relation vectorielle

$$a = ((\alpha_j^i))\, b$$

est équivalente à

$$b = ((\beta_j^i))\, a .$$

Remarque. Soient des polynômes $P_n(x)$ et $Q_n(x)$ qui s'annulent pour $x = 0$, $n \neq 0$, et soient Δ et D les opérateurs de dérivation associés. Ce que nous venons de dire montre que sont inverses l'une de l'autre les matrices suivantes :

$$\left\| \begin{matrix} Q_0(0) & 0 & 0 & \ldots \\ Q_1(0) & \dfrac{\Delta Q_1(0)}{1!} & 0 & \ldots \\ Q_2(0) & \dfrac{\Delta Q_2(0)}{1!} & \dfrac{\Delta^2 Q_2(0)}{2!} & \ldots \end{matrix} \right\| \quad \text{et} \quad \left\| \begin{matrix} P_0(0) & 0 & 0 & \ldots \\ P_1(0) & \dfrac{DP_1(0)}{1!} & 0 & \ldots \\ P_2(0) & \dfrac{DP_2(0)}{1!} & \dfrac{D^2P_2(0)}{2!} & \ldots \end{matrix} \right\| .$$

Formules binomiales inverses

Si l'on pose $x = y + 1$, on a, d'après la formule du binôme :

$$x^n = (y + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (x - 1)^k .$$

De la même façon, on a :

$$(x-1)^n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} x^k .$$

D'après le premier théorème de l'inversion, on voit que *si des nombres* $a_0, a_1, a_2, \ldots, b_0, b_1, b_2, \ldots$ *vérifient*

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k ,$$

alors on a :

$$b_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_k .$$

En particulier, on a vu (formule 1, § 10, Chap. 1) :

$$n^p = \sum_{k=0}^{n} \binom{n}{k} (k!\, S_p^k)$$

(en posant arbitrairement $S_p^0 = 0$).

On obtient donc

$$(n!\, S_p^n) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^p$$

ou

$$\boxed{S_n^m = \frac{1}{m!} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} k^n} \quad \text{(Formule de STIRLING)} .$$

Formules inverses de Stirling

On a vu (Chap. 1, § 5) que les nombres de Stirling de première espèce s_k^n sont définis par

$$[x]_n = \sum_{k=1}^{n} s_n^k x^k .$$

On a également vu (Chap. 1, § 10) la formule :

$$x^n = \sum_{k=1}^{n} S_n^k [x]_k .$$

Le premier théorème de l'inversion montre alors que *si des nombres* $a_1, a_2, \ldots, b_1, b_2, \ldots$ *vérifient*

$$a_n = \sum_{k=1}^{n} s_n^k b_k ,$$

alors on a :

$$b_n = \sum_{k=1}^{n} S_n^k a_k .$$

Formules inverses de Lah

$[-x]_n$ étant un polynôme de degré n, on peut le développer en série

$$[-x_n] = L_n^1[x]_1 + \cdots + L_n^n[x]_n .$$

Les nombres L_n^k s'appellent les *nombres de Lah* ; en changeant x en $-x$, on obtient :

$$[x]_n = L_n^1[-x]_1 + \cdots + L_n^n[-x]_n .$$

En vertu du premier théorème de l'inversion, on obtient :

$$a_n = \sum_{k=1}^{n} L_n^k b_k \Leftrightarrow b_n = \sum_{k=1}^{n} L_n^k a_k .$$

§ 2. *Fonction de Möbius*

Nous allons ici généraliser le théorème d'inversion précédent. La présentation suivante de la fonction de Möbius est due essentiellement à G. C. ROTA [15], qui a proposé d'en faire la base de la Combinatoire, avec un point de vue unifié.

Considérons un ensemble quelconque X, muni d'une relation d'ordre notée $\leqslant$; on a donc par définition :

$$\begin{cases} x \leqslant x \\ x \leqslant y, y \leqslant x \Rightarrow x = y \\ x \leqslant y, y \leqslant z \Rightarrow x \leqslant z . \end{cases}$$

On peut supposer que l'ensemble X possède un minorant universel, noté 0 ; c'est-à-dire

$$0 \leqslant x \qquad (x \in X)$$

(si cet élément n'existait pas, on peut toujours l'ajouter).

Supposons enfin que, pour tout $x, y \in X$, l'intervalle

$$[x, y] = \{ u \,/\, u \in X, u \geqslant x, u \leqslant y \}$$

soit un ensemble fini. Par la suite, un ensemble X muni d'une relation d'ordre vérifiant les conditions énoncées ci-dessus sera appelé un ensemble *ordonné localement fini.*

On peut prendre pour X, par exemple, l'ensemble des entiers $\geqslant 0$, avec la relation

$$x \leqslant y \quad \Leftrightarrow \quad x \text{ plus petit ou égal à } y .$$

On peut prendre pour X l'ensemble des entiers $\geqslant 1$, avec la relation

$$x \leqslant y \quad \Leftrightarrow \quad x \text{ est un diviseur de } y .$$

Nous rencontrerons bien d'autres exemples ultérieurement.

On posera comme d'habitude : $x < y$ si $x \leqslant y$ et $x \neq y$; on pose $x \geqslant y$ si $y \leqslant x$.

Soit X un ensemble ordonné localement fini.

Soit A l'ensemble des fonctions $f(x, y)$ définies pour $x, y \in X$ à valeurs réelles (ou, plus généralement, à valeurs sur un corps quelconque), telles que

$$\begin{aligned} f(x, y) &\neq 0 \quad \text{pour} \quad x = y \\ f(x, y) &= 0 \quad \text{si} \quad x \not\leqslant y . \end{aligned}$$

Définissons sur A un produit, noté $*$, par :

$$f * g(x, y) = \sum_{x \leqslant u \leqslant y} f(x, u)\, g(u, y) .$$

La somme est prise pour tout point u de l'intervalle fini $[x, y]$.

L'ensemble A, avec le produit $*$, est appelé le *groupe des fonctions arithmétiques*. Montrons en effet que c'est un « groupe ».

PROPOSITION 1. *Le produit $*$ est associatif, c'est-à-dire* :

$$(f * g) * h = f * (g * h) .$$

En effet, on a

$$\begin{aligned} [(f * g) * h](x, z) &= \sum_{x \leqslant y \leqslant z} h(y, z) \sum_{x \leqslant u \leqslant y} f(x, u)\, g(u, y) \\ &= \sum_{x \leqslant u \leqslant y \leqslant z} f(x, u)\, g(u, y)\, h(y, z) . \end{aligned}$$

On trouverait la même expression si l'on formait

$$[f * (g * h)](x, z) .$$

PROPOSITION 2. *Le produit $*$ admet un élément unité, qui est la fonction de Kronecker* :

$$\delta(x, y) = \begin{cases} 1 & \text{si} \quad x = y , \\ 0 & \text{si} \quad x \neq y . \end{cases}$$

En effet, on a

$$[f * \delta](x, y) = \sum_{x \leqslant u \leqslant y} f(x, u)\, \delta(u, y) = f(x, y) .$$

PROPOSITION 3. *Si $f \in A$, il existe un inverse à gauche $f^{-1} \in A$,* (c'est-à-dire tel que $f^{-1}f = \delta$) ; *pour un point x donné, $f^{-1}(x, y)$ est défini par induction sur y par*

(1) Si $y = x$: $\quad f^{-1}(x, y) = \dfrac{1}{f(x, x)}$;

(2) Si $y > x$: $\quad f^{-1}(x, y) = \dfrac{-1}{f(y, y)} \sum_{x \leqslant u < y} f^{-1}(x, u) f(u, y)$.

En effet, on a d'après (1) :

$$f^{-1} * f(x, x) = f^{-1}(x, x) f(x, x) = 1 .$$

Si $x < y$, on a d'après (2) :

$$f^{-1} * f(x, y) = \sum_{x \leqslant u < y} f^{-1}(x, u) f(u, y) + f^{-1}(x, y) f(y, y) = 0 ,$$

on a donc bien $f^{-1} * f = \delta$.

Les propositions 1, 2, 3 montrent que A est un groupe ; en effet, on sait que si tout élément α d'un monoïde possède un inverse à gauche α^{-1}, cet élément est aussi un inverse à droite ; car on a :

$$\alpha\alpha^{-1} = f = \delta f = f^{-1} ff = f^{-1} \alpha\alpha^{-1} \alpha\alpha^{-1} = f^{-1} \alpha\delta\alpha^{-1} = f^{-1} f = \delta .$$

On pourrait aussi constater que A est un anneau, qui possède de nombreuses propriétés remarquables (Cf. SMITH [18], CARLITZ [1]).

En ce qui nous concerne, la propriété importante est

$$f = g * \alpha \quad \Rightarrow \quad g = f * \alpha^{-1} ,$$

c'est-à-dire : à toute fonction $\alpha(x, y)$, telle que $\alpha(x, x) \neq 0$ et $\alpha(x, y) = 0$ si $x \nleqslant y$, on peut faire correspondre une fonction $\beta(x, y)$ avec les mêmes propriétés et telle que

$$f(0, x) = \sum_{0 \leqslant u \leqslant x} \alpha(u, x)\, g(0, u)$$

entraîne

$$g(0, x) = \sum_{0 \leqslant u \leqslant x} \beta(u, x) f(0, u) .$$

X étant un ensemble localement fini, on appelle *fonction de Riemann* la fonction

$$\xi(x, y) = \begin{cases} 1 & \text{si} \quad x \leqslant y , \\ 0 & \text{sinon} . \end{cases}$$

On appelle *fonction de Möbius* la fonction μ définie par induction (pour tout $y \geqslant x$) par :

$$\mu(x, x) = 1 ,$$

$$\mu(x, y) = - \sum_{x \leqslant t < y} \mu(x, t) .$$

Les fonctions ξ et μ étant inverses, au sens du théorème précédent, on a :

THÉORÈME D'INVERSION DE MÖBIUS. *Soit X un ensemble localement fini, $f(x)$ et $g(x)$ des fonctions définies sur X, avec :*

$$f(x) = \sum_{0 \leqslant u \leqslant x} g(u) \qquad (x \in X) .$$

Alors on a :

$$g(x) = \sum_{0 \leqslant u \leqslant x} \mu(u, x) f(u) \qquad (x \in X) .$$

Exemple 1. Prenons pour X l'ensemble des entiers positifs, avec la relation $\leqslant$ définie par : $k \leqslant n$ si « k est plus petit ou égal à n ».

Cherchons à inverser :

$$f(n) = \sum_{k=1}^{n} g(k) .$$

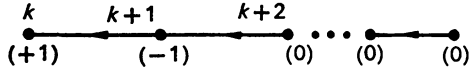


FIG. 1.

La fonction de Möbius est définie pour tout $n \geqslant k$ par :

$$\mu(k, n) = \begin{cases} 1 & \text{si} \quad n = k \\ -1 & \text{si} \quad n = k + 1 \\ 0 & \text{si} \quad n = k + 2, k + 3, \ldots \end{cases}$$

On trouve alors :

$$g(n) = f(n) - f(n - 1) .$$

Exemple 2. Prenons pour X l'ensemble des entiers positifs, avec la relation $\leqslant$ définie par :

$$y \leqslant x \quad \text{si} \quad y \text{ divise } x \quad (\text{ou : } y/x) .$$

On se propose d'inverser :

$$f(n) = \sum_{d/n} g(d) .$$

Cherchons la fonction de Möbius $\mu(d, n)$ sur le graphe de la figure 2.

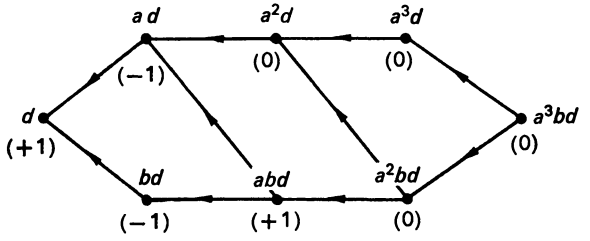


FIG. 2.

On trouve immédiatement :

$$\mu(d, n) = \begin{cases} +1 & \text{si} \quad n = d , \\ (-1)^k & \text{si} \quad n = p_1 p_2 \dots p_k d , \quad \text{les } p_i \text{ étant premiers} \neq 1 \text{ et tous différents.} \\ 0 & \text{sinon} . \end{cases}$$

Alors

$$g(n) = \sum_{d/n} \mu(d, n) f(d) .$$

C'est la fonction $\mu(d, n)$ — plus souvent écrire $\mu\left(\frac{d}{n}\right)$ — qui a été trouvée par Möbius en 1832 pour étudier la répartition des nombres premiers.

Exemple 3. A étant un ensemble fini, inversons la formule :

$$f(A) = \sum_{S \subset A} g(S)$$

X est ici le treillis des parties de A avec la relation d'ordre $\subset$ (inclusion).

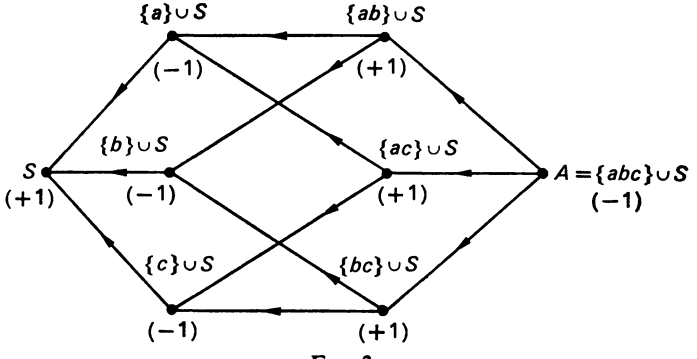


FIG. 3.

On trouve alors :

$$\mu(S, A) = (-1)^{|A|-|S|} .$$

D'où la formule

$$g(A) = \sum_{S \subset A} (-1)^{|A|-|S|} f(S) .$$

Exemple 4. Considérons un ensemble A et une partition

$$\mathscr{A} = (A_1, A_2, ..., A_k)$$

de A ; on a donc par définition :

$$\begin{cases} A_i \neq \varnothing \\ i \neq j \Rightarrow A_i \cap A_j = \varnothing \\ \bigcup A_i = A \end{cases}$$

On pose $\mathscr{B} < \mathscr{A}$ ($\mathscr{B}$ est une « sous-partition » de $\mathscr{A}$) si

$$\left.\begin{array}{l} B_j \cap A_i \neq \varnothing \\ B_j \in \mathscr{B} \\ A_i \in \mathscr{A} \end{array}\right\} \Rightarrow B_j \subset A_i$$

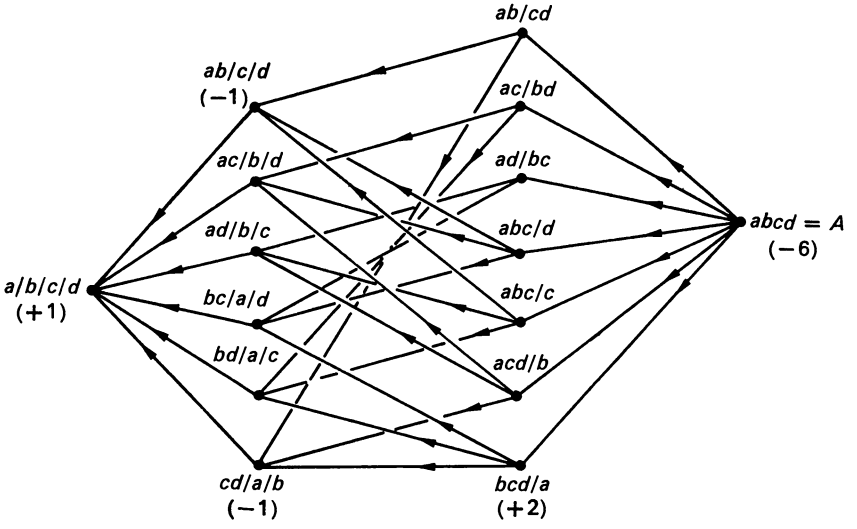


FIG. 4.

Si $\mathscr{A}$ est une partition de A, défini par p classes $A_1, A_2, ..., A_p$, et si $\mathscr{B}$ est une sous-partition de $\mathscr{A}$, chaque A_i contient n_i classes de $\mathscr{B}$. On trouve alors

$$\mu(\mathscr{B}, \mathscr{A}) = (-1)^{p+n_1+n_2+\cdots+n_p} (n_1 - 1)! (n_2 - 1)! ... (n_p - 1)!$$

Cette formule, trouvée par M. P. SCHÜTZENBERGER [16], a été reformulée par R. FRUCHT et G. C. ROTA [15] en vue de différentes applications.

Application: Le problème des mots circulaires (C. MOREAU, [11]). Un *alphabet* est un ensemble de m symboles distincts $a_1, a_2, ..., a_m$, appelés *lettres*; un *mot de longueur n* est une application φ de $X = \{ 1, 2, ..., n \}$ dans

$$A = \{ a_1, a_2, ..., a_m \} .$$

Si deux mots φ et φ' vérifient

$$\varphi'(i) = \varphi(i + p) \qquad (i = 1, 2, ..., n)$$

(les sommes étant modulo n), on dira qu'ils sont *équivalents* ou qu'ils constituent le même « mot circulaire ». On se propose ici de dénombrer les mots circulaires de n lettres.

Si un mot φ est tel que $\varphi(i + p) = \varphi(i)$ pour tout i, on dit que p est une *période* de φ ; la plus petite période p ($1 \leqslant p \leqslant n$) est appelée la *période primitive* de φ. Par exemple, le mot *abcabcabc* est de période primitive $p = 3$.

Il est évident qu'une période p est nécessairement un diviseur de n. Soit $M(p)$ le nombre de mots circulaires de période primitive p ; il lui correspond $pM(p)$ mots différents, donc le nombre total de mots est

$$m^n = \sum_{p/n} pM(p) .$$

Inversons cette formule en considérant la fonction de Möbius $\mu(d, n)$ du treillis des diviseurs (Exemple 2) :

$$\mu(d, n) = \begin{cases} (-1)^k & \text{si } n = p_1, p_2, ..., p_k, d \text{ où les } p_i \text{ sont des nombres premiers} \neq 1 \text{ et différents entre eux,} \\ 0 & \text{sinon .} \end{cases}$$

On obtient donc

$$pM(p) = \sum_{q/p} \mu(q, p)\, m^q .$$

Le nombre total de mots circulaires est donc [1]

$$\sum_{p/n} M(p) = \sum_{p/n} \frac{1}{p} \sum_{q/p} \mu(q, p)\, m^q .$$

---

[1] Signalons que la même formule peut être étendue pour prouver les théorèmes de POLYA démontrés par des méthodes directes au chapitre 5 ; voir G. C. ROTA, Enumération under Group Action, à paraître dans le *Journal of Combinatorial Theory*, 1969.

Une généralisation de ce problème célèbre en théorie de l'information est le problème des dictionnaires « comma-free ». Un *dictionnaire comma-free* est un ensemble de mots de n lettres vérifiant la propriété suivante : si l'on prend deux mots quelconques du dictionnaire, il n'y a pas d'entier k ($1 \leqslant k < n$) tel que les $n - k$ dernières lettres du premier mot, suivi des k premières lettres du second mot constituant un mot du dictionnaire. Le problème que l'on se pose est de déterminer un dictionnaire avec un nombre maximum de mots.

Pour calculer plus aisément la fonction de Möbius, on peut s'aider de différents théorèmes, comme le suivant :

THÉORÈME DE PH. HALL. *Supposons que l'ensemble ordonné* $(X, \leqslant)$ *soit un demi-treillis — c'est-à-dire pour tout* $a, b \in X$, *il existe un plus petit majorant* c (*appelé la conjonction de* a *et* b *et noté* $c = a \vee b$) *tel que* :

$$c \geqslant a, b$$
$$x \geqslant a, b \quad \Rightarrow \quad x \geqslant c .$$

Si $x > y$, *et si* x *n'est pas la conjonction de prédécesseurs de* y, *alors on a*

$$\mu(y, x) = 0 .$$

Supposons que x ne soit pas la conjonction de prédécesseurs de y, c'est-à-dire d'éléments de l'ensemble :

$$\{ z \mid z \in X, z \geqslant y, \text{ il n'existe pas de } t \text{ avec } z > t > y \} .$$

Soient $a_1, a_2, \ldots, a_k$ les prédécesseurs de y qui sont $\leqslant x$, et considérons leur conjonction $b = a_1 \vee a_2 \vee \cdots \vee a_k$:

on a $y \leqslant b \leqslant x$ (car $a, a' \leqslant x$ entraîne $a \vee a' \leqslant x$),
on a $b \neq x$ (car sinon x serait une conjonction de prédécesseurs de y),
on a $b \neq y$ (car le graphe est sans circuits).

Si l'on suppose le théorème vrai pour $\mu(y, z)$ avec $z < x$, il est encore vrai pour $\mu(y, x)$, car

$$-\mu(y, x) = \sum_{z \in [y, x[} \mu(y, z) = \sum_{y \leqslant z < b} \mu(y, z) + \mu(y, b) + 0 = 0$$

C. Q. F. D.

(on peut vérifier ce résultat sur les exemples précédents).

§ 3. *Formules du crible*

Nous allons considérer ici, sur un ensemble X fini, une fonction $m(x) \geqslant 0$, définie pour tout $x \in X$, et appelée la *mesure* (ou le poids) *de l'élément* x. Si $A \subset X$, on pose

$$m(A) = \sum_{x \in A} m(x) \qquad \text{si} \qquad A \neq \varnothing ;$$

$$m(\varnothing) = 0 \qquad \text{si} \qquad A = \varnothing ;$$

$m(A)$ est appelé la *mesure de l'ensemble* A.

Par exemple : si $m(x) = 1$ pour tout $x \in X$, on a $m(A) = |A|$, *cardinalité* de l'ensemble A ; si $m(x)$ est une distribution de probabilités sur des événements et A l'ensemble des événements ayant une certaine propriété, $m(A)$ désigne la probabilité d'obtenir cette propriété.

Formule 1

Si $A, B \subset X$, et si l'on désigne par $\overline{A}$ le complémentaire $X - A$, on a :

$$\boxed{\begin{aligned} m(\overline{A}) &= m(X) - m(A) \\ m(\overline{A \cup B}) &= m(\overline{A} \cap \overline{B}) \\ m(\overline{A \cap B}) &= m(\overline{A} \cup \overline{B}) \end{aligned}}$$

(évident).

Formule 2

Soient $A_i \, (i \in \{1, 2, ..., q\} = Q)$ *des sous-ensembles de* X, *et posons* :

$$\overline{m}(K) = m\Big(\bigcup_{i \in K} A_i\Big) \quad \text{si} \quad K \neq \varnothing, \quad = 0 \quad \text{si} \quad K = \varnothing$$

$$\underline{m}(K) = m\Big(\bigcap_{i \in K} A_i\Big) \quad \text{si} \quad K \neq \varnothing, \quad = 0 \quad \text{si} \quad K = \varnothing .$$

On a

$$\boxed{\overline{m}(Q) = \sum_{K \subset Q} (-1)^{|K|+1} \underline{m}(K) .}$$

Par exemple, pour $q = 2$, on a évidemment :

$$m(A_1 \cup A_2) = m(A_1) + m(A_2) - m(A_1 \cap A_2) .$$

Démontrons la formule 2 par induction sur $q = |Q|$; supposons la vraie pour des sous-ensembles $A_1, A_2, \ldots, A_{q-1}$ et montrons qu'elle est vraie pour les sous-ensembles $A_1, A_2, \ldots, A_{q-1}, A_q$. On a :

$$m(A_1 \cup A_2 \cup \cdots \cup A_{q-1} \cup A_q) =$$

$$= m(A_1 \cup \cdots \cup A_{q-1}) + m(A_q) - m((A_i \cup \cdots \cup A_{q-1}) \cap A_q)$$

$$= m(A_1 \cup \cdots \cup A_{q-1}) + m(A_q) - m\Big(\bigcup_{i<q} A_i \cap A_q\Big)$$

$$= \sum_{i<q} m(A_i) - \sum_{i<j<q} m(A_i \cap A_j) + \sum_{i<j<k<q} m(A_i \cap A_j \cap A_k) - \ldots$$

$$+ m(A_q) - \sum_{i<q} m(A_i \cap A_q) + \sum_{i<j<q} m(A_i \cap A_j \cap A_q) - \ldots$$

$$= \sum_{i\leqslant q} m(A_i) - \sum_{i<j\leqslant q} m(A_i \cap A_j) + \sum_{i<j<k\leqslant q} m(A_i \cap A_j \cap A_k) - \ldots$$

Formule 3

Soient $A_i (i \in \{1, 2, \ldots, q\} = Q)$ *des sous-ensembles de X. On a :*

$$\underline{m}(Q) = \sum_{K\subset Q} (-1)^{|K|+1}\, \overline{m}(K).$$

La fonction de Möbius est ici

$$\mu(I, J) = (-1)^{|J|-|I|}.$$

On inverse la formule 2 par le théorème d'inversion de Möbius :

$$(-1)^{|Q|+1}\, \underline{m}(Q) = \sum_{K\subset Q} (-1)^{|K|-|Q|}\, \overline{m}(K).$$

D'où

$$\underline{m}(Q) = \sum_{K\subset Q} (-1)^{|K|+1}\, \overline{m}(K) = \sum_{i\leqslant q} m(A_i) - \sum_{i<j\leqslant q} m(A_i \cup A_j) + \cdots$$

Cette formule 3 peut aussi s'obtenir à partir de la formule 2 par passage au complémentaire.

FORMULE DE SYLVESTER. *Soient* $A_1, A_2, \ldots, A_q \subset X$ *et posons* $\underline{m}(K) = \underline{m}(K)$ si $K \neq \varnothing$, *et* $\underline{m}(\varnothing) = X$; *l'ensemble des éléments de X qui n'appartiennent à aucun des ensembles* A_i *a pour mesure* :

$$T_q^0 = \sum_{k=0}^{q} (-1)^k \sum_{\substack{K\subset Q \\ |K|=k}} \underline{m}(K).$$

Ceci se déduit immédiatement de la formule 2 car :

$$T_q^0 = m\Big(\bigcap_{i\in Q} \overline{A}_i\Big) = m\Big(\overline{\bigcup_{i\in Q} A_i}\Big) = m(X) - m\Big(\bigcup_{i\in Q} A_i\Big) =$$

$$= \underline{\underline{m}}(\varnothing) - \sum_{\substack{K\subset Q\\ K\neq\varnothing}} (-1)^{|K|+1}\, \underline{\underline{m}}(K)\,.$$

FORMULE DU CRIBLE. *Soient $A_1, A_2, \ldots, A_q \subset X$; l'ensemble des éléments de X qui appartiennent à exactement p des ensembles A_i a pour mesure :*

$$\boxed{T_q^p = \sum_{k=p}^{q} (-1)^{k-p}\binom{k}{p} \sum_{\substack{K\subset Q\\ |K|=k}} \underline{\underline{m}}(K)\,.}$$

En considérant un ensemble $P \subset Q$ de p éléments, et en remplaçant X par $\bigcap_{i\in P} A_i$, et A_j par $A_j \cap \bigcap_{i\in P} A_i$, la formule de Sylvester donne :

$$m\Big(\bigcap_{i\in P} A_i \cap \bigcap_{j\in Q-P} \overline{A}_j\Big) = m\Big(\bigcap_{i\in P} A_i\Big) - \sum_{\substack{K\supset P\\ |K|=p+1}} m\Big(\bigcap_{i\in K} A_i\Big) + \cdots$$

$$= \sum_{K\supset P} (-1)^{|K|-|P|}\, \underline{\underline{m}}(K)\,.$$

On peut donc écrire :

$$T_q^p = \sum_{|P|=p} m\Big(\bigcap_{i\in P} A_i \cap \bigcap_{j\in Q-P} \overline{A}_i\Big) = \sum_{|P|=p} \sum_{K\supset P} (-1)^{|K|-|P|}\, \underline{\underline{m}}(K)$$

$$= \sum_{\substack{K\subset Q\\ |K|\geqslant p}} \sum_{\substack{P\subset K\\ |P|=p}} (-1)^{|K|-|P|}\, \underline{\underline{m}}(K) = \sum_{k=p}^{q} (-1)^{k-p} \sum_{\substack{K\subset Q\\ |K|=k}} \underline{\underline{m}}(K)\binom{k}{p}\,.$$

D'où la formule annoncée.

Remarquons que cette formule contient la formule de Sylvester (cas où $p = 0$).

Les formules du Crible correspondent à une méthode d'énumération très générale (appelée la méthode du Crible, en raison du « Crible d'Eratosthène », permettant de construire de proche en proche le tableau des nombres premiers). Quand on veut énumérer les éléments qui n'appartiennent à aucun des ensembles $A_1, A_2, \ldots, A_q$, on part du tableau de tous les éléments, on élimine tous ceux de A_1, puis tous ceux de A_2, et ..., de façon à obtenir finalement $\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_q$.

APPLICATION 1. (Montmort). *Le problème des rencontres.* On considère une permutation

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

en tant qu'application bijective de $\{1, 2, ..., n\}$ dans lui-même, et l'on dira que φ admet une *coïncidence* (ou une *rencontre*) en i si $\varphi(i) = i$.

Par exemple, la permutation

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 7 & 5 & 6 & 4 \end{pmatrix}$$

présente 3 coïncidences, en 3, 5 et 6.

On se propose de chercher le nombre de permutations d'ordre n qui comportent exactement p coïncidences.

Cherchons d'abord le nombre $P(n)$ de permutations sans coïncidences, et désignons par A_i l'ensemble des $(n-1)!$ permutations qui comportent une coïncidence en i.

La formule de Sylvester donne :

$$P(n) = |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n| = \underline{\underline{m}}(\varnothing) - \sum_{|K|=1} \underline{\underline{m}}(K) + \sum_{|K|=2} \underline{\underline{m}}(K) - \cdots$$

si $|K| = k$, on a :

$$\underline{\underline{m}}(K) = \left| \bigcap_{i \in K} A_i \right| = (n-k)!\,.$$

D'où

$$P(n) = n! - \binom{n}{1}(n-1)! + \cdots + (-1)^k \binom{n}{k}(n-k)! + \cdots + (-1)^n \binom{n}{n}$$

ou encore

$$\boxed{P(n) = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{(-1)^k}{k!} + \cdots + (-1)^n \frac{1}{n!}\right]}\,.$$

Le nombre de permutations avec exactement p coïncidences est

$$P^p(n) = \binom{n}{p} P(n-p)\,.$$

Il suffit donc de calculer $P(n)$, ce qui est obtenu facilement par les formules suivantes :

$$P(1) = 0$$

$$P(n) = nP(n-1) + (-1)^n\,.$$

D'où le tableau :

$P^p(n)$	$p = 0$	$p = 1$	$p = 2$	$p = 3$	...
$n = 1$	0	1			
$n = 2$	1	0	1		
$n = 3$	2	3	0	1	
$n = 4$	9	8	6	0	
$n = 5$	44	45	20	10	
...					

APPLICATION 2. (Touchard) : *Problème des Ménages.*

Le problème des ménages consiste à compter le nombre de façons $T(n)$ de placer n maris (numérotés 1, 2, ..., n) et leurs épouses respectives (numérotées $\underline{1}$, $\underline{2}$, ..., $\underline{n}$) autour d'une table circulaire, de façon que chaque homme ait deux femmes pour voisines, aucune des deux n'étant sa propre femme. Une bijection φ définit une disposition de la façon suivante : la place de l'homme 1 ; à sa droite la femme $\varphi(1)$; à sa droite, l'homme 2 ; à sa droite, la femme $\varphi(2)$; etc. Pour $i = 1, 2, ..., n$, désignons par A_{2i-1} l'ensemble des bijections φ avec $\varphi(i) = \underline{i}$.

Si $i \neq 1$, désignons par A_{2i} l'ensemble des bijections φ avec $\varphi(i) = \underline{i+1}$ (pour $i = n$, A_{2n} désigne l'ensemble des bijections φ, avec $\varphi(n) = \underline{1}$). La réponse au problème des ménages est d'après la formule de Sylvester :

$$T(n) = \left| \bigcap_{i \in Q} \overline{A}_i \right| = \sum_{K \subset Q} (-1)^{|K|} \underline{\underline{m}}(K)$$

où $Q = \{1, 2, ..., 2n\}$.

Pour $|K| = k$, on a

$$\underline{\underline{m}}(K) = \left| \bigcap_{i \in K} A_i \right| = (n-k)! \quad \text{si } K \text{ ne comporte pas deux entiers consécutifs de la suite } (1, 2, ..., 2n, 1) ;$$

$$= 0 \quad \text{sinon.}$$

Or on a vu au chapitre 1 (§ 8, nombres de FIBONACCI) que le nombre d'ensembles K de cardinalité k, ne comportant pas deux entiers consécutifs de la suite $(1, 2, ..., 2n, 1)$, est

$$f^*(2n, k) = \frac{2n}{2n-k} \binom{2n-k}{k}.$$

D'où la formule :

$$T(n) = n! - \frac{2n}{2n-1}\binom{2n-1}{1}(n-1)! + \\ + \frac{2n}{2n-2}\binom{2n-2}{2}(n-2)! + \cdots + (-1)^n \frac{2n}{n}\binom{n}{n}0!$$

On voit de même que le nombre de façons de ranger les n maris et leurs épouses de façon qu'il y ait exactement p maris assis à côté de leurs femmes est

$$T^p(n) = \sum_{k=p}^{2n} (-1)^{k-p}\binom{k}{p}\frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!$$

APPLICATION 3. (Euler) : *Dénombrement des nombres premiers.*

Si $n > 0$, proposons-nous de chercher le nombre $\varphi(n)$ d'entiers $\leqslant n$ qui sont premiers avec n.

On peut écrire

$$n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_q^{\alpha_q},$$

avec $p_1, p_2, \ldots, p_q$ premiers $\neq 1$ et différents entre eux.

Soit A_i l'ensemble des entiers $\leqslant n$ qui sont des multiples de p_i ; on a

$$|A_i| = \frac{n}{p_i},$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, \text{ etc.}$$

Prenons X = ensemble des entiers $\leqslant n$, $m(A)$ = cardinalité de A ; la formule de Sylvester donne alors :

$$\varphi(n) = |X| - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k) + \cdots$$

$$= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \cdots$$

D'où finalement :

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_q}\right)} \quad \text{(fonction d'Euler)}.$$

§ 4. *Problèmes de rangements*

Soit X un ensemble de n objets, dont certains sont indistinguables entre eux ; si deux objets x et y sont indistinguables, on dira qu'ils sont *de la même espèce* ; si les espèces déterminent sur X une partition du type $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$, on dira que X est une *collection d'objets du type* $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$.

On se propose ici de ranger les objets dans des boîtes $a_1, a_2, \dots, a_m$, dont certaines sont indistinguables entre elles, et forment une collection de boîtes du type $1^{\mu_1} 2^{\mu_2} \dots m^{\mu_m}$.

Un rangement est donc une application φ de X dans A ; on dira que deux rangements sont équivalents s'ils sont indistinguables, c'est-à-dire si l'un se déduit de l'autre par permutation d'objets de même espèce ou de boîtes de même espèce ; on appelle *schémas* les classes de cette équivalence.

On se propose ici de calculer le nombre de schémas de rangements d'une collection d'objets de type $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ dans une collection de boîtes de type $1^{\mu_1} 2^{\mu_2} \dots m^{\mu_m}$, soit

$$R'(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; 1^{\mu_1} 2^{\mu_2} \dots m^{\mu_m}) .$$

On désignera également par

$$R(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; \ 1^{\mu_1} 2^{\mu_2} \dots m^{\mu_m})$$

le nombre de schémas de rangements qui ne laissent aucune boîte vide.

Remarquons que si l'on écrit $m_1 m_2 \dots m_p$ un partage de l'entier m en parts $m_1, m_2, \dots, m_p$, on a :

$$R'(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; m_1 m_2 \dots m_p) = \sum_{\substack{0 \leqslant k_1 \leqslant m_1 \\ 0 \leqslant k_2 \leqslant m_2 \\ \dots\dots\dots\dots}} R(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; \ k_1 k_2 \dots k_p) .$$

D'autre part, si l'on désigne par $\mu(k_1 k_2 \dots k_p, m_1 m_2 \dots m_p)$ la fonction de Mobius (chap. 3, § 2) pour le treillis des p-uples (Chap. 1, § 9), on a :

$$R(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; \ m_1 m_2 \dots m_p) =$$

$$\sum_{\substack{0 \leqslant k_1 \leqslant m_1 \\ 0 \leqslant k_2 \leqslant m_2 \\ \dots\dots\dots\dots}} \mu(k_1 k_2 \dots k_p, m_1 m_2 \dots m_p) \times R'(1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} ; \ k_1 k_2 \dots k_p) .$$

Une méthode générale pour calculer R et R' sera donnée au chapitre 5 ; néanmoins, on peut obtenir directement ces nombres par une formule simple dans un grand nombre de cas.

PROPOSITION 1. *On a*

$$R(1^n ; m) = S_n^m \text{ (nombre de Stirling)}$$
$$R'(1^n ; m) = S_n^1 + S_n^2 + \dots + S_n^m .$$

En effet, $R(1^n ; m)$ est le nombre de partitions d'un ensemble de n objets tous distincts en m classes.

PROPOSITION 2. *On a*

$$R(1^n ; 1^m) = m!\, S_n^m$$

$$R'(1^n ; 1^m) = n^m .$$

Car R est le nombre d'applications surjectives de X dans A, et R' le nombre total d'applications.

PROPOSITION 3. *On a*

$$R(n ; m) = P_n^m \text{ (nombre de partages de } n \text{ en } m \text{ parts)}$$

$$R'(n ; m) = P_n^1 + P_n^2 + \cdots + P_n^m$$

(évident).

PROPOSITION 4. *On a*

$$R(n ; 1^m) = \binom{n-1}{m-1}$$

$$R'(n ; 1^m) = \binom{n+m-1}{n} .$$

R' est le nombre d'additions $u_1 + u_2 + \cdots + u_m$ réalisant le total n avec m entiers $\geqslant 0$, qui est (Cf. Chapitre 1, § 7) :

$$R'(n ; 1^m) = \frac{[n+1]^{m-1}}{(m-1)!} = \binom{n+m-1}{n} .$$

R est le nombre d'additions $u_1 + u_2 + \cdots + u_m$ réalisant le total n avec m entiers > 0, deux additions étant comme précédemment considérées comme distinctes si elles diffèrent par la nature des u_i ou par leur ordre ; si l'on pose $s_k = u_1 + u_2 + \cdots + u_k$, chaque addition est complètement déterminée par des nombres $s_1, s_2, \ldots, s_{m-1}$, avec :

$$1 \leqslant s_1 < s_2 < \cdots < s_{m-1} \leqslant n - 1 .$$

D'où la première formule.

THÉORÈME. *On a*

$$R(1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n} ; 1^m) = \sum_{k=0}^{m} (-1)^{n-k} \binom{m}{k} \binom{k}{1}^{\lambda_1} \binom{k+1}{2}^{\lambda_2} \ldots \binom{k+n-1}{n}^{\lambda_n}$$

$$R'(1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n} ; 1^m) = \binom{m}{1}^{\lambda_1} \binom{m+1}{2}^{\lambda_2} \ldots \binom{m+n-1}{n}^{\lambda_n} .$$

Si l'on admet la possibilité de laisser des boîtes vides, on peut d'abord ranger les n_1 objets de la première espèce, puis les n_2 objets de la deuxième espèce, etc... ce qui représente un nombre de possibilités :

$$R'(n_1\, n_2 \ldots ; 1^m) = R'(n_1 ; 1^m)\, R'(n_2 ; 1^m) \ldots$$
$$= \binom{n_1 + m - 1}{n_1} \binom{n_2 + m - 1}{n_2} \ldots$$

D'où la seconde formule.

Pour démontrer la première, remarquons que l'on a, en notant R_k ou $R(K)$ le nombre de rangements dans un sous-ensemble $K \subset A$ de boîtes (avec $|K| = k$) :

$$R'_m = \sum_{K \subset A} R(K) = \sum_{k=0}^{m} \binom{m}{k} R_k .$$

D'après la formule binomiale inverse (Chap. 3, § 1), on a donc :

$$R_m = \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} R'_k .$$

D'où la première formule.

APPLICATION. *Nombre de partages parfaits d'un entier s.*

Considérons une boîte de poids contenant

t_1 poids d'un kilogramme

t_2 poids de deux kilogrammes, etc. ,

avec $t_1 + 2\, t_2 + \cdots = s$.

On dira que le partage $1^{t_1}\, 2^{t_2} \ldots s^{t_s}$ est *parfait* si la boîte de poids permet d'effectuer tout pesage depuis 1 kilo jusqu'à s kilos, et cela d'une façon unique.

On se propose de chercher combien il y a de partages parfaits de s comprenant m espèces de poids.

On a le résultat :

Considérons la décomposition en nombres premiers :

$$s + 1 = \prod_{i=0}^{\lambda_1} p_i^1 \left(\prod_{i=0}^{\lambda_2} p_i^2 \right)^2 \left(\prod_{i=0}^{\lambda_2} p_i^3 \right)^3 \ldots$$

où $p_0^k = 1$ *pour tout* k, *et où pour* $i \neq 0$, *les* p_i^k *sont des nombres premiers tous différents entre eux et différents de* 1.

Le nombre de partages parfaits de s qui comprennent m espèces de poids est égal à $R(1^{\lambda_1}\, 2^{\lambda_2} \ldots n^{\lambda_n} ; 1^m)$.

Posons

$$s + 1 = p'_1 p'_2 \dots p'_n$$

où les p'_i sont des nombres premiers différents de 1.

Au moins une des parts du partage cherché doit être égale à 1 ; si le nombre de 1 dans ce partage est $a_1 - 1$, la part suivante du partage doit être égale à a_1 ; si le nombre de parts égales à a_1 est $a_2 - 1$, la part suivante doit être égale à $(a_1\, a_2)$ et il y en aura $(a_3 - 1)$; etc. On peut alors écrire :

$$s = a_1 - 1 + (a_2 - 1)\, a_1 + (a_3 - 1)\, a_1\, a_2 + (a_4 - 1)\, a_1\, a_2\, a_3 + \cdots \\ \cdots + (a_m - 1)\, a_1\, a_2 \dots a_{m-1}$$

ou :

$$s + 1 = a_1\, a_2 \dots a_m = p'_1\, p'_2 \dots p'_n .$$

Une séquence $(a_1, a_2, \dots, a_m)$ détermine complètement le partage parfait de s ; comme les p' sont premiers $\neq 1$, le nombre de séquences possibles est bien

$$R(1^{\lambda_1}\, 2^{\lambda_2} \dots n^{\lambda_n} ; 1^m) .$$

D'où le résultat.

§ 5 . *Dénombrement des arbres*

Rappelons les définitions usuelles de la Théorie des Graphes : un graphe est défini par un ensemble X de *sommets* et un ensemble d'*arcs*, ou couples (x, y) de sommets ; une *arête* est un ensemble $\{ x, y \}$ de deux sommets reliés par un arc. Leur ensemble sera dénoté par U.

Un *chemin* est une séquence d'*arcs* telle que l'extrémité terminale de chaque arc est l'extrémité initiale du suivant ; un chemin qui part d'un sommet pour y aboutir est un *circuit*. Deux sommets a et b appartiennent à la même *composante fortement connexe* s'il existe un chemin allant de a à b, et un chemin allant de b à a. Une *chaîne* est une séquence d'arêtes distinctes, chacune étant jointe à la précédente par une extrémité et à la suivante par l'autre extrémité.

Une *chaîne* qui part d'un sommet x pour y aboutir est un *cycle*. Deux sommets a et b appartiennent à la même *composante connexe* s'il existe une chaîne allant de a à b.

Un graphe partiel de (X, U) est un graphe (X, V) avec $V \subset U$; un sous-graphe de (X, U) est un graphe ayant pour ensemble de sommets $S \subset X$, et pour arêtes toutes les arêtes de U qui relient deux points de S. Si G est un graphe avec n sommets, m arcs, p composantes connexes, rappelons que *le nombre de cycles indépendants est*

$$k(G) = m - n + p .$$

Pour une démonstration, cf. [22].

Un arbre est un graphe connexe sans cycles ; plus exactement, on a :

THÉORÈME 1. *Soit $H = (X, U)$ un graphe d'ordre $|X| = n \geqslant 2$; les propriétés suivantes sont équivalentes pour caractériser un arbre :*

(1) *H est connexe et sans cycles ;*

(2) *H est sans cycles et admet $n - 1$ arêtes ;*

(3) *H est connexe et admet $n - 1$ arêtes ;*

(4) *H est sans cycles et en ajoutant une arête, on crée un cycle (et un seul) ;*

(5) *H est connexe, et si on supprime une arête quelconque, il n'est plus connexe ;*

(6) *tout couple de sommets est relié par une chaîne et une seule.*

(1) $\Rightarrow$ (2), car en désignant par p le nombre de composantes connexes, m le nombre d'arêtes, on a

$$p = 1, \quad k(H) = m - n + p = 0 .$$

donc $m = n - p = n - 1$.

(2) $\Rightarrow$ (3), car $k(H) = 0$, $m = n - 1$, donc

$$p = k(H) - m + n = 1 ,$$

et H est connexe.

(3) $\Rightarrow$ (4), car $p = 1$, $m = n - 1$, donc

$$k(H) = m - n + p = 0 ,$$

H est sans cycles ; en outre, si l'on ajoute une arête, $k(H)$ devient égal à 1, donc il y a un cycle et un seul.

(4) $\Rightarrow$ (5), car si H n'était pas connexe, deux sommets a et b n'étant pas connectés, on ne peut en ajoutant l'arête $\{ a, b \}$ créer un cycle ; donc $p = 1$. $k(H) = 0$, d'où $m = n - 1$. D'autre part, en supprimant une arête, on a

$$m' = n' - 2, \qquad k(H') = 0 ,$$

d'où

$$p' = k(H') - m' + n' = 2 ,$$

et H' n'est donc plus connexe.

(5) $\Rightarrow$ (6), car pour deux sommets a et b, il existe une chaîne allant de l'un à l'autre (car H est connexe), et il n'en peut exister deux (car la suppression d'une arête n'appartenant qu'à la seconde chaîne ne disconnecterait pas le graphe).

(6) $\Rightarrow$ (1), car si H admettait un cycle, au moins un couple de sommets serait relié par deux chaînes distinctes.

COROLLAIRE. *Un graphe $G = (X, U)$ admet un graphe partiel qui soit un arbre si et seulement si il est connexe.*

Si G n'est pas connexe, aucun de ses graphes partiels n'est connexe, donc G n'admet pas d'arbres partiels.

Si G est connexe, cherchons s'il existe un arc dont la suppression ne disconnexe pas le graphe. Si un tel arc n'existe pas, G est un arbre, en vertu de la propriété (5) ; et si un tel arc existe, on le supprimera, et on cherchera un nouvel arc à éliminer, etc.

Dès qu'on ne pourra plus supprimer d'arcs, on aura un arbre dont l'ensemble des sommets est précisément X.

Ce résultat donne un algorithme simple pour construire un arbre H dans un graphe connexe G.

Etant donné un graphe (X, U) le *degré* d'un sommet $a \in X$ est par définition le nombre $d(a)$ d'arêtes qui ont une extrémité au point a. Un sommet x de l'arbre tel que $d(x) = 1$ est appelé un sommet *pendant*.

THÉORÈME 2 (J. Moon [9]). *Désignons par* $T(n ; d_1, d_2, ..., d_n)$ *le nombre d'arbres dont les sommets sont des points donnés* $x_1, x_2, ..., x_n$ *et dont les degrés sont des nombres donnés* $d(x_1) = d_1, d(x_2) = d_2, ..., d(x_n) = d_n$; *on a* :

$$T(n ; d_1, d_2, ..., d_n) = \binom{n-2}{d_1 - 1, d_2 - 1, ..., d_n - 1} .$$

1° Remarquons au préalable que la somme des degrés est deux fois le nombre des arêtes, soit $2(n-1)$ pour un arbre (d'après le théorème 1). Donc $T \neq 0$ seulement si

$$\sum_{i=1}^{n} (d_i - 1) = 2(n-1) - n = n - 2 .$$

On peut supposer, sans rien changer à l'énoncé, que $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n$; comme l'égalité ci-dessus implique que $d_n = 1$, le sommet x_n est un sommet « pendant » de l'arbre.

2° Montrons que

$$T(n ; d_1, d_2, ..., d_n) = \sum_{i \,/\, d_i \geqslant 2} T(n-1 ; d_1, d_2, ..., d_i - 1, ..., d_{n-1}) .$$

Formons la liste $\mathscr{C}_i$ de tous les arbres ayant des sommets $x_1, x_2, ..., x_n$ et des degrés $d(x_k) = d_k$, et tel que le sommet pendant x_n soit relié à x_i. Si $d_i \geqslant 2$, on a

$$|\mathscr{C}_i| = T(n-1 ; d_1, d_2, ..., d_i - 1, ..., d_{n-1}) .$$

Comme la liste de tous les arbres est la réunion des listes $\mathscr{C}_i$ (pour $d_i \geqslant 2$), on a bien l'égalité du (2°).

3° La formule de l'énoncé est triviale pour $n = 3$; supposons donc $n \geqslant 3$. Supposons-la démontrée pour $n - 1$; on a donc

$$\begin{aligned} T(n\,;\,d_1, d_2, \ldots, d_n) &= \sum_{i\,/\,d_i \geqslant 2} T(n-1\,;\,d_1, d_2, \ldots, d_i - 1, \ldots, d_n) \\ &= \sum_{i\,/\,d_i \geqslant 2} \binom{n-3}{d_1 - 1, d_2 - 1, \ldots, d_i - 2, \ldots, d_{n-1} - 1} \\ &= \binom{n-2}{d_1 - 1, d_2 - 1, \ldots, d_{n-1} - 1} \\ &= \binom{n-2}{d_1 - 1, d_2 - 1, \ldots, d_n - 1}. \end{aligned}$$

(D'après la conséquence 1, § 9, Chap. 1).

COROLLAIRE 1 (Menon [7]). *Des nombres $d_1, d_2, \ldots, d_n \geqslant 1$ sont les degrés d'un arbre si et seulement si*

$$\sum_{i=1}^{n} d_i = 2(n-1).$$

En effet, cette condition équivaut à $T(n\,;\,d_1, d_2, \ldots, d_n) \neq 0$.

COROLLAIRE 2 (Formule de Cayley). *Le nombre d'arbres de sommets $x_1, x_2, \ldots, x_n$ est n^{n-2}.*

En effet, c'est

$$\sum_{d_1, \ldots, d_n \geqslant 1} \binom{n-2}{d_1 - 1, d_2 - 1, \ldots, d_n - 1} = (1 + 1 + \cdots + 1)^{n-2} = n^{n-2}.$$

COROLLAIRE 3 (Clarke [3]). *Le nombre d'arbres de sommets $x_1, x_2, \ldots, x_n$ et pour lesquels $d(x_1) = k$ est :*

$$\binom{n-2}{k-1}(n-1)^{n-k-1}.$$

En effet, le nombre cherché est

$$\begin{aligned} &\sum_{d_2, d_3, \ldots, d_n} \binom{n-2}{k-1, d_2 - 1, d_3 - 1, \ldots, d_n - 1} = \\ &= \frac{(n-2)!}{(k-1)!\,(n-k-1)!} \sum_{d_2, d_3, \ldots, d_n \geqslant 1} \binom{n-k-1}{d_2 - 1, d_3 - 1, \ldots, d_n - 1} \\ &= \binom{n-2}{k-1}(n-1)^{n-k-1} \end{aligned}$$

(en faisant toutes les variables égales à 1 dans la formule de multinôme).

COROLLAIRE 4 (Lemme de Moon [9]). *Soient*

$$H_1 = (X_1, U_1),\ H_2 = (X_2, U_2),\ \ldots\ H_p = (X_p, U_p),$$

des arbres disjoints d'ordres $|X_i| = n_i$; *le nombre d'arbres d'ordre n ayant pour ensemble de sommets la réunion des* X_i, *et qui admettent les* H_i *comme sous-graphes, est*

$$T(H_1, H_2, \ldots, H_p) = n_1\, n_2 \ldots n_p\, n^{p-2}\,.$$

En effet, supposons provisoirement que chaque ensemble X_i soit « *contracté* », c'est-à-dire assimilé à un sommet unique $\bar{x}_i$; le nombre d'arbres $\bar{H}$ avec $d(\bar{x}_i) = d_i$ est donc

$$\binom{p-2}{d_1 - 1,\ d_2 - 1,\ \ldots,\ d_p - 1}.$$

A chacun de ces arbres $\bar{H}$ correspondent $(n_1)^{d_1}\,(n_2)^{d_2} \ldots (n_p)^{d_p}$ arbres H du graphe initial. Donc

$$T(H_1, H_2, \ldots, H_p) = \sum_{d_1, d_2, \ldots, d_p \geqslant 1} \binom{p-2}{d_1 - 1,\ d_2 - 1,\ \ldots,\ d_p - 1} (n_1)^{d_1}\,(n_2)^{d_2} \ldots (n_p)^{d_p}$$

$$= n_1\, n_2 \ldots n_p (n_1 + n_2 + \cdots + n_p)^{p-2}\,.$$

D'où la formule.

COROLLAIRE 5 (Cayley). *Le nombre de graphes, de sommets* $x_1, x_2, \ldots, x_n$, *formés de p arbres disjoints, et pour lesquels* $x_1, x_2, \ldots, x_p$ *appartiennent à p arbres différents, est*

$$T'(n\,;\,p) = p\, n^{n-p-1}\,.$$

Formons la liste $\mathscr{C}$ des arbres de sommets $x_0, x_1, x_2, \ldots, x_n$ avec $d(x_0) = p$; d'après le corollaire 3, on a

$$|\mathscr{C}| = \binom{n-1}{p-1} n^{n-p}\,.$$

Si $P \subset \{1, 2, \ldots, n\}$, et $|P| = p$, désignons par $\mathscr{C}_P$ la liste des arbres de $\mathscr{C}$ pour lesquels, pour tout $i \in P$, le sommet x_i est relié à x_0. On a

$$|\mathscr{C}| = \sum_P |\mathscr{C}_P| = \sum_P T'(n\,;\,p)\,.$$

D'où :

$$\binom{n-1}{p-1} n^{n-p} = \binom{n}{p} T'(n\,;\,p)\,.$$

D'où :

$$T'(n\,;\,p) = \frac{(n-1)!}{(p-1)!\,(n-p)!} \cdot \frac{p!(n-p)!}{n!}\, n^{n-p} = p n^{n-p-1}\,.$$

C. Q. F. D.

Soit $X = \{ x_1, x_2, ..., x_n \}$ un ensemble de n points, $U = \{ u_1, u_2, ..., u_q \}$ un ensemble de q arêtes qui joignent des paires de points dans X. On se propose maintenant de chercher le nombre $T(X, U)$ d'arbres que l'on peut former avec les sommets $x_1, x_2, ..., x_n$ et les arêtes qui joignent des paires de points dans X mais qui n'appartiennent pas à U. Il existe une formule générale utilisant la théorie des déterminants (Cf. BERGE [22], Ch. 16), mais pour les cas particuliers que nous considérons ici, elle s'avère sans beaucoup d'utilité. Soit (X, V) un graphe de n sommets, q arêtes, et p composantes connexes ayant respectivement $n_1, n_2, ..., n_p$ sommets.

Posons :

$$v(V) = \begin{cases} 0 & \text{si le graphe } (X, V) \text{ possède un cycle} \\ n_1\, n_2 \ldots n_p & \text{sinon}\,. \end{cases}$$

THÉORÈME 3 (Temperley [19]). *Le nombre d'arbres dont les sommets sont les points de X et dont les arêtes n'appartiennent pas à U est* :

$$T(X, U) = n^{n-2} \sum_{V \subset U} v(V) \left(\frac{-1}{n}\right)^{|V|}\,.$$

En effet, si $v \in U$, désignons par A_v l'ensemble des arbres qui utilisent l'arête v.

Si (X, V) est acyclique et a p composantes connexes, le lemme de Moon indique que le nombre d'arbres qui utilisent toutes les arêtes de V est :

$$\left| \bigcap_{v \in V} A_v \right| = v(V)\, n^{p-2} = v(V)\, n^{n-|V|-2}\,.$$

Si (X, V) possède un cycle, cette formule est encore vraie, car les deux membres de l'égalité sont nuls.

La formule de Sylvester donne donc :

$$T(X, U) = n^{n-2} + \sum_{\substack{V \subset U \\ V \neq \varnothing}} (-1)^{|V|}\, v(V)\, n^{n-2-|V|} = n^{n-2} \sum_{V \subset U} v(V) \left(\frac{-1}{n}\right)^{|V|}\,.$$

COROLLAIRE 1 (Weinberg [21]). *Si U est un ensemble de q arêtes deux à deux disjointes, on a*

$$T(X, U) = n^{n-2} \left(1 - \frac{2}{n}\right)^q\,.$$

En effet, dans ce cas, on a pour $V \subset U$,

$$v(V) = 2^{|V|},$$

$$T(X, U) = n^{n-2} \sum_{k=0}^{q} 2^k \binom{q}{k} \left(\frac{-1}{n}\right)^k = n^{n-2} \left(1 - \frac{2}{n}\right)^q.$$

COROLLAIRE 2 (O'Neil [12]). *Si U consiste en q arêtes ayant toutes une extrémité commune x_1, on a*

$$T(X, U) = n^{n-2} \left(1 - \frac{1}{n}\right)^{q-1} \left(1 - \frac{q+1}{n}\right).$$

En effet, on a

$$\sum_{V \subset U} v(V) \left(\frac{-1}{n}\right)^{|V|} = \sum_{k=0}^{q} (k+1) \binom{q}{k} \left(\frac{-1}{n}\right)^k$$

$$= \sum_{k=0}^{q} \binom{q}{k} \left(\frac{-1}{n}\right)^k + \sum_{k-1=0}^{q-1} \left(\frac{-q}{n}\right) \binom{q-1}{k-1} \left(\frac{-1}{n}\right)^{k-1}$$

$$= \left(1 - \frac{1}{n}\right)^q - \frac{q}{n} \left(1 - \frac{1}{n}\right)^{q-1} = \left(1 - \frac{1}{n}\right)^{q-1} \left(1 - \frac{1}{n} - \frac{q}{n}\right).$$

COROLLAIRE 3 (Austin). *Si U est l'ensemble des arêtes qui joignent de toutes les façons possibles les points de $S \subset X$ (avec $|S| = s$), c'est-à-dire si (S, U) est un « graphe complet », on a*

$$T(X, U) = n^{n-2} \left(1 - \frac{s}{n}\right)^{s-1}.$$

Si $\mathscr{V}_p$ désigne la famille des $V \subset U$ tels que (S, V) est acyclique avec p composantes connexes, on peut écrire :

$$\sum_{V \subset U} v(V) \left(\frac{-1}{n}\right)^{|V|} = \sum_{p=1}^{s} \left(\frac{-1}{n}\right)^{s-p} \sum_{V \in \mathscr{V}_p} v(V).$$

Si $P \subset S$, $|P| = p$, $V \in \mathscr{V}_p$, considérons l'ensemble des triplets (S, V, P) qui sont des graphes acycliques avec un sommet de P distingué dans chaque composante connexe.

D'après le corollaire 5 du théorème 2, on sait que

$$|\{(S, V, P) / V \in \mathscr{V}_p\}| = p s^{s-p-1}.$$

Donc

$$\sum_{V \in \mathscr{V}_p} v(V) = \sum_{V \in \mathscr{V}_p} \left| \{ (S, V, P) / P \subset S, |P| = p \} \right|$$

$$= \left| \{ (S, V, P) / P \subset S, |P| = p ; V \in \mathscr{V}_p \} \right|$$

$$= \sum_{\substack{P \subset S \\ |P| = p}} p s^{s-p-1} = \binom{s}{p} p s^{s-p-1}$$

Donc

$$\sum v(V) \left(\frac{-1}{n}\right)^{|V|} = \sum_{p=1}^{s} \left(\frac{-1}{n}\right)^{s-p} \binom{s}{p} p s^{s-p-1}$$

$$= \sum_{p-1=0}^{s-1} \left(\frac{-s}{n}\right)^{s-p} \binom{s-1}{p-1} = \left(1 - \frac{s}{n}\right)^{s-1} .$$

COROLLAIRE 4 (Scoin, Glicksman [4]). *Si le graphe (X, U) est la réunion de deux graphes complets disjoints (S, V) et (T, W), avec $|S| = s$, $|T| = t$, on a*

$$T(X, U) = s^{t-1} t^{s-1} .$$

En effet, d'après le théorème 3, on voit que :

$$\frac{T(X, V \cup W)}{n^{n-2}} = \frac{T(X, V)}{n^{n-2}} \cdot \frac{T(X, W)}{n^{n-2}} .$$

Donc, d'après le corollaire 3 :

$$T(X, U) = n^{n-2} \left(1 - \frac{s}{n}\right)^{s-1} \left(1 - \frac{t}{n}\right)^{t-1}$$

$$= (s + t)^{s+t-2} \left(\frac{s + t - s}{s + t}\right)^{s-1} \left(\frac{s + t - t}{s + t}\right)^{t-1} = s^{t-1} t^{s-1} .$$

COROLLAIRE 5 (Moon). *Si U consiste en $m - 1$ arêtes formant une chaîne ouverte avec un ensemble de m sommets $Y \subset X$, on a*

$$T(X, U) = n^{n-2} \sum_{p=1}^{m} \binom{m + p - 1}{m - p} \left(\frac{-1}{n}\right)^{m-p} .$$

En effet, si $V \subset U$ détermine un graphe (Y, V) avec p composantes connexes, on a

$$|V| = |Y| - p = m - p .$$

Si $m_1, m_2, \ldots, m_p$ sont les nombres de sommets pour ces différentes composantes connexes, on a $m_1 + m_2 + \cdots + m_p = m$.

Donc, pour $|V| = m - p$, il y a autant de graphes (Y, V) qu'il y a de façons de réaliser le total m en additionnant des entiers $m_1, m_2, \ldots, m_p > 0$, d'où :

$$\sum_{V \subset U} v(V) \left(\frac{-1}{n}\right)^{|V|} = \sum_{p=1}^{m} \left(\frac{-1}{n}\right)^{m-p} \sum_{\substack{|V|=m-p \\ V \subset U}} v(V) =$$

$$= \sum_{p=1}^{m} \left(\frac{-1}{n}\right)^{m-p} \sum_{\substack{m_1, m_2, \ldots > 0 \\ m_1 + m_2 + \cdots + m_p = m}} m_1 \, m_2 \ldots m_p \, .$$

Cette dernière somme est égale au coefficient de x^m dans le développement

$$(x + 2x^2 + 3x^3 + \cdots)^p = x^p (1 - x)^{-2p} \, .$$

D'après la formule du binôme, ce coefficient est égal à :

$$(-1)^{m-p} \frac{-2p(-2p-1)(-2p-2)\ldots\left(-2p-(m-p-1)\right)}{(m-p)!} =$$

$$= \frac{(m+p-1)(m+p-2)\ldots(2p+1)\,2p}{(m-p)!}$$

$$= \binom{m+p-1}{m-p} \, .$$

D'où la formule.

4

Groupes de permutations

§ 1. *Généralités*

Une *permutation de degré n* est une application bijective

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

de l'ensemble $X = \{ 1, 2, ..., n \}$ dans lui-même.

Comme toute application, elle est sujette à deux interprétations. Si X est une suite d'objets 1, 2, ..., n rangés dans des places données, *effectuer la permutation* φ sur ces objets, c'est remplacer l'objet en i par l'objet $k_i = \varphi(i)$. Le n-uple $k_1\, k_2 \dots k_n$, qui est le résultat de cette permutation, est parfois appelé le *réarrangement* de la suite 1 2 ... n dans la permutation φ.

THÉORÈME 1. *Les permutations de degré n forment un groupe* S_n, *appelé le groupe symétrique à n variables.*

Considérons deux permutations f et g de l'ensemble $X = \{ 1, 2, ..., n \}$, par exemple :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ k_1 & k_2 & k_3 & k_4 & k_5 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

Par définition, le *produit* $f.g$ est l'opération qui consiste à effectuer la permutation g, puis la permutation f ; autrement dit, on a :

$$f.g(i) = f\big(g(i)\big).$$

On peut écrire

$$f.g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ k_1 & k_2 & k_3 & k_4 & k_5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 5 & 3 & 4 \\ k_2 & k_1 & k_5 & k_3 & k_4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ k_2 & k_1 & k_5 & k_3 & k_4 \end{pmatrix}.$$

En effet,

$$f.g(1) = f(g1) = f(2) = k_2\,,$$
$$f.g(2) = f(g2) = f(1) = k_1\,, \text{ etc}\,.$$

On a changé l'ordre des colonnes dans le premier facteur f de façon à reproduire en haut le réarrangement g, et on a gardé la deuxième ligne du premier facteur avec la première ligne du deuxième facteur.

Il est à noter qu'en général, on a :

$$(f.g) \neq (g.f)\,;$$

par exemple,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Dire que l'ensemble S_n des permutations de degré n, avec le produit ainsi défini, forme un *groupe*, c'est dire que l'on a les axiomes suivants :

(I) *Associativité* : On a toujours :

$$f.(g.h) = (f.g).h\,,$$

et la permutation obtenue se notera plus simplement $f.g.h$.

(II) *Existence d'un élément unité* : Il existe dans S_n un élément, noté e, tel que

$$f.e = e.f = f\,.$$

(III) *Existence des éléments inverses.* Pour tout $f \in S_n$, il existe un élément de S_n, noté f^{-1}, tel que

$$f.f^{-1} = f^{-1}.f = e\,.$$

L'axiome (I) est évident car :

$$[f.(g.h)]\,(i) = f\{\,g[h(i)]\,\} = [(f.g).h]\,(i)\,.$$

L'axiome (II) se vérifie en prenant pour e la *permutation identique*, qui ne déplace aucun objet, c'est-à-dire :

$$e = \begin{pmatrix} 1\ 2\ \dots\ n \\ 1\ 2\ \dots\ n \end{pmatrix}.$$

On a bien

$$f.e(i) = f(i) \qquad e.f(i) = e[f(i)] = f(i).$$

L'inverse de la permutation

$$f = \begin{pmatrix} k_1\ k_2\ \dots\ k_n \\ p_1\ p_2\ \dots\ p_n \end{pmatrix}$$

est la permutation

$$f^{-1} = \begin{pmatrix} p_1\ p_2\ \dots\ p_n \\ k_1\ k_2\ \dots\ k_n \end{pmatrix}$$

obtenue en plaçant en haut la première ligne de f, et en bas la seconde ligne de f.

En effet, on a :

$$(f.f^{-1})\, p_i = fk_i = p_i,$$
$$(f^{-1}.f)\, k_i = f^{-1}\, p_i = k_i.$$

Donc, on a bien :

$$f.f^{-1} = f^{-1}.f = e.$$

Remarque 1. Si n est un entier > 0, l'application f^n défini par

$$f^n(i) = \overbrace{f.f \dots f}^{n}(i)$$

est une permutation ; cette permutation s'appelle la *puissance n-ième de f*. On posera

$$f^0 = e.$$

De même, l'application f^{-n} définie par

$$f^{-n}(i) = \overbrace{f^{-1}.f^{-1}.\dots.f^{-1}}^{n}(i)$$

est une permutation de X appelée la *puissance moins n-ième de f*.

Un sous-ensemble G de S_n est dit un *groupe de permutations* (ou un *sous-groupe de* S_n) si les éléments de G, avec la multiplication définie plus haut, vérifient encore les axiomes (I), (II), (III).

Rappelons ici :

THÉORÈME 2. *Un sous-ensemble H d'un groupe fini G est un sous-groupe de G si et seulement si on a la condition*

$$h, h' \in H \Rightarrow h.h' \in H .$$

(*Dans ce cas, on notera* $H \subseteq G$.)

Ceci est une propriété bien connue des complexes finis. En effet, si $g \in H$, considérons l'application φ de H dans lui-même définie par

$$\varphi(h) = g.h \qquad (h \in H) .$$

Elle est injective, car

$$g.h = g.h' \quad \Rightarrow \quad h = g^{-1}(g.h) = g^{-1}(gh') = h' .$$

Comme H est fini, elle est bijective, donc :

$$\varphi(H) = \{ g.h \mid h \in H \} = H .$$

Donc, il existe dans H un élément h_0 tel que $g = g.h_0$, d'où

$$h_0 = g^{-1} g = e , \quad \text{élément unité de } G .$$

De même, il existe dans H un élément h_1 tel que $e = g.h_1$, d'où

$$h_1 = g^{-1} , \quad \text{élément inverse de } g \text{ dans } G .$$

H, qui contient l'élément unité e et l'inverse h^{-1} de tout $h \in H$ est bien un sous-groupe de G.

Exemple. Considérons le groupe S_3 des permutations sur $\{ 1, 2, 3 \}$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} , \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} , \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} ,$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} , \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} , \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} .$$

Formons la table de Pythagore pour la multiplication de ces permutations ; on a

$$c.f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = a$$

$$f.c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = b , \text{ etc.}$$

On trouve alors la table :

$x.y$	$y=$ e	a	b	c	d	f
$x=e$	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

On voit sur cette table que :

e engendre $\{e\}$
a engendre $\{e, a\}$
b engendre $\{e, b\}$
c engendre $\{e, c\}$
d engendre $\{e, d, f\}$
f engendre $\{e, d, f\}$

Les sous-groupes de S_3 sont donc obtenus, sous forme de treillis, par le tableau suivant :

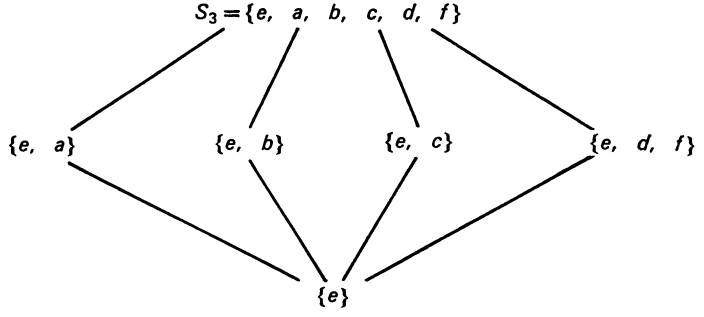


FIG. 1.

Un autre concept important en théorie des groupes est celui de « sous-groupe normal ». Si G est un groupe de permutations, un sous-groupe $H \subseteq G$ est un *sous-groupe normal* de G si

$$H.g = g.H \qquad \text{pour tout } g \in G.$$

Le symbole $H.g$ signifie : l'ensemble des éléments de la forme $x = h.g$, où $h \in H$. On peut aussi définir un sous-groupe normal par :

$$H = gHg^{-1} \qquad \text{pour tout } g \in G \ .$$

Une propriété importante des sous-groupes normaux est : si $A \subseteq G$, $H \subseteq G$, et si H est normal dans G, on a :

$$A.H = \bigcup_{a \in A} a.H = \bigcup_{a \in A} H.a = H.A \ .$$

Autrement dit, *les sous-groupes normaux commutent avec tous les sous-groupes de G.*

Exemple. Considérons encore les sous-groupes de $G = S_3$ (Fig. 1). Il est évident que S_3 est un sous-groupe normal de S_3, car

$$a.S_3 = \{ a.x \mid x \in S_3 \} = S_3 = S_3.a \ .$$

De même, $\{ e \}$ est un sous-groupe normal de S_3, car $a.e = e.a$; ni $\{ e, a \}$, ni $\{ e, b \}$ ne sont normaux dans S_3, car

$$\{ e, a \}.\{ e, c \} = \{ e, c, a, d \} \ ; \ \{ e, c \}.\{ e, a \} = \{ e, a, c, f \} \ .$$

On a donc

$$A.H \neq H.A \ .$$

On vérifie de même que $\{ e, b \}$ n'est pas normal dans S_3. Cherchons si $\{ e, d, f \}$ est normal.

$$x.d.x^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \beta & \gamma & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \end{pmatrix} = d \quad \text{ou} \quad f \ ;$$

$$x.f.x^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \gamma & \alpha & \beta \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix} = d \quad \text{ou} \quad f \ .$$

Donc il est normal, et S_3 contient seulement trois sous-groupes normaux : S_3, $\{ e \}$ et $\{ e, d, f \}$.

THÉORÈME 3. 1° *Si $H \subseteq G$ est un sous-groupe d'un groupe G, les différents ensembles de la forme* :

$$H.a = \{ h.a \mid h \in H \} \ ,$$

constituent une partition de l'ensemble G, et l'ensemble des classes s'appelle l'ensemble quotient G/H ; l'on a

$$| G/H | = \frac{| G |}{| H |}.$$

2° *Si de plus H est normal dans G, l'ensemble quotient forme un groupe avec la multiplication* :

$$K.K' = \{ x.x' \mid x \in K, x' \in K' \}.$$

L'application $\varphi(a) = H.a$ *de X dans G/H est une homomorphie, c'est-à-dire* :

$$\varphi(a.b) = \varphi(a).\varphi(b).$$

1° Les ensembles $H.a$ forment une partition de G, car la relation $x \in H.g$ est une relation d'équivalence :

$$x \in H.x \quad \text{car } x = e.x,$$
$$x \in H.y \Rightarrow x = h.y \Rightarrow y = h^{-1}.x \Rightarrow y \in H.x.$$
$$\left.\begin{matrix} x \in H.y \\ y \in H.z \end{matrix}\right\} \Rightarrow \left.\begin{matrix} x = h.y \\ y = h'.z \end{matrix}\right\} \Rightarrow x = h.h'.z \Rightarrow x \in H.z.$$

La classe Ha a exactement $| H |$ éléments, car

$$h.a = h'.a \quad \Rightarrow \quad h = h'.a.a^{-1} = h'.$$

Donc le nombre de classes est

$$| G/H | = \frac{| G |}{| H |}.$$

2° Si H est normal dans G, G/H est un groupe, car

$$(Ha).(Hb) = H^2.a.b = H.a.b,$$

$$(Ha).(He) = H^2.a = H.a,$$

$$(Ha).(Ha^{-1}) = H.a.a^{-1}.H = H^2 = H = (H.e).$$

De plus on voit sur ces formules que l'application $\varphi(a) = H.a$ de G sur G/H est une homomorphie.

COROLLAIRE (Théorème de Lagrange). *Si* $H \subseteq G$, *alors* $| H |$ *divise* $| G |$. En effet $| G/H | = \frac{| G |}{| H |}$ est un nombre entier.

Par exemple, pour S_3 qui est d'ordre $| S_3 | = 3 ! = 6$, les seuls sous-groupes possibles sont d'ordre 1, 2, 3, 6 ; c'est ce que l'on a vérifié plus haut. Il est à remarquer que la réciproque de ce théorème n'est pas vraie :

Dans S_4, un groupe G est formé par les permutations :

$$e,\quad a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\quad b=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\quad c=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\quad d=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},$$

$$f=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\quad g=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},\quad h=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\quad i=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},$$

$$j=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\quad k=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\quad l=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}.$$

Il est d'ordre 12, et cependant ne contient aucun sous-groupe d'ordre 6. Par contre, on peut démontrer « Si G est un groupe d'ordre $p^m q$, p premier avec q, pour tout $i \leqslant m$ il existe un sous-groupe H d'ordre $p^i q$ ». C'est le théorème de Sylow (que nous n'aurons pas à utiliser ici).

§ 2. *Cycles d'une permutation*

A chaque permutation f, on peut associer un *graphe*, en représentant par des points 1, 2, ..., n les éléments de X, et en joignant les points i et $f(i)$ par un « arc », c'est-à-dire une ligne continue avec une flèche allant de i vers $f(i)$.

Comme f est bijective, de chaque sommet i du graphe part une flèche et une seule, et vers chaque sommet arrive une flèche et une seule. Si l'on considère la suite $k, f(k), f^2(k), f^3(k)$, ..., on retombera sur un élément déjà écrit (car X est fini) ; le premier élément que l'on retrouve sera k, car si c'était $i \neq k$, le point i serait le point d'arrivée de deux flèches distinctes.

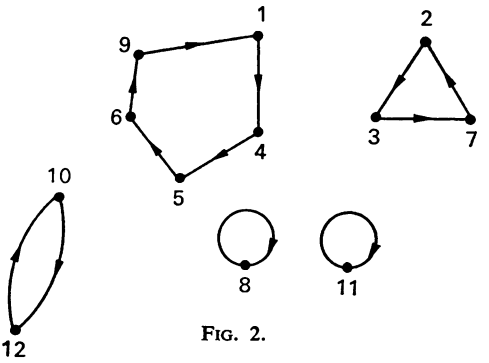


FIG. 2.

Exemple.

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\4&3&7&5&6&9&2&8&1&12&11&10\end{pmatrix}$$

Chaque composante connexe de ce graphe est un cycle, et les différents cycles partitionnent X.

On note plus souvent la permutation f de la façon suivante :

$$f=[1\ 4\ 5\ 6\ 9]\ [2\ 3\ 7]\ [10\ 12]\ [8]\ [11]\,.$$

Cette notation permet en effet de retrouver l'application f d'une façon évidente.

On appelle *permutation circulaire* une permutation f qui ne comporte qu'un cycle de plusieurs éléments.

Par exemple

$$f = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,1\,2\,4\,5\,6 \end{pmatrix}$$

est une permutation circulaire des éléments 1, 2, 3 que l'on note plus simplement :

$$f = [1\ 3\ 2]\ [4]\ [5]\ [6] \quad \text{ou même} \quad f = [1\ 3\ 2]\,.$$

Remarque. La notation indiquée permet aussi d'écrire directement le produit de plusieurs permutations.

Considérons par exemple les permutations :

$$f = [1\ 3\ 4]\ [2\ 6]$$
$$g = [1\ 5\ 2]\ [3\ 6\ 4]$$
$$h = [1\ 4\ 5\ 6]$$

L'on se propose d'effectuer le produit :

$$f.g.h = [1\ 3\ 4]\ [2\ 6]\ [1\ 5\ 2]\ [3\ 6\ 4]\ [1\ 4\ 5\ 6]\,.$$

On commence à considérer le chiffre 1, et l'on suit sa transformation dans les différents facteurs en allant de la droite vers la gauche :

$$1 \to 4 \to 3 \to 3 \to 3 \to 4\,.$$

On écrit alors [1 4...] et l'on suit de même les transformations du 4 :

$$4 \to 5 \to 5 \to 2 \to 6 \to 6\,.$$

On écrit [1 4 6...], et l'on suit la transformation du 6 :

$$6 \to 1 \to 1 \to 5 \to 5 \to 5\,.$$

Puis :

$$5 \to 6 \to 4 \to 4 \to 4 \to 1\,,$$

le premier cycle est donc bouclé : [1 4 6 5] ; on commence alors le deuxième cycle en partant du plus petit chiffre non encore écrit, c'est-à-dire 2 :

$$2 \to 2 \to 2 \to 1 \to 1 \to 3$$
$$3 \to 3 \to 6 \to 6 \to 2 \to 2\,.$$

D'où

$$fgh = [1\ 4\ 5\ 6]\ [2\ 3]\,.$$

Soit G un sous-groupe de S_n. Deux permutations s et t sont dites *conjuguées dans* G s'il existe un élément $g \in G$ tel que $s = gtg^{-1}$. Le fait d'être conjugués dans G est une relation d'équivalence, car :

1° réflexive : $s = ese^{-1}$; $e \in G$;

2° symétrique : $s = gtg^{-1} \Rightarrow t = g^{-1} s g = h s h^{-1}$; $h = g^{-1} \in G$;

3° transitive : $\left.\begin{array}{l} s = gtg^{-1} \\ t = huh^{-1} \end{array}\right\} \Rightarrow s = ghuh^{-1} g^{-1} = (gh)\, u\, (gh)^{-1}$; $gh \in G$.

Nous allons nous intéresser aux classes de cette équivalence.

THÉORÈME 1. *Deux permutations s et t sont conjuguées dans S_n si et seulement si leurs cycles sont en même nombre k et de mêmes longueurs n_i* (pour $i = 1, 2, \ldots, k$).

1° Soit

$$t = [a_{11}\, a_{12} \ldots a_{1i}]\, [a_{21}\, a_{22} \ldots a_{2j}] \ldots [a_{m1}\, a_{m2} \ldots a_{mk}]$$

une permutation écrite par cycles avec la convention définie plus haut.

Si g est une permutation de S_n, et si l'on pose $b_{pq} = g(a_{pq})$, la permutation $s = gtg^{-1}$ vérifie

$$s(b_{11}) = gtg^{-1}(b_{11}) = g.t(a_{11}) = g(a_{12}) = b_{12}\,;$$

on a donc

$$s = [b_{11}\, b_{12} \ldots b_{1i}]\, [b_{21}\, b_{22} \ldots b_{2j}] \ldots [n_{m1}\, b_{m2} \ldots b_{mk}]\,.$$

Donc deux permutations conjuguées se décomposent en cycles de mêmes longueurs.

2° Inversement, dans ce cas, s et t sont conjuguées, en prenant la permutation g définie par $g(a_{pq}) = b_{pq}$.

Exemple. Pour $n = 3$, on trouve trois classes de conjuguées, correspondant aux trois partages de n :

$$\begin{cases} 3 = 1 + 1 + 1 \\ 3 = 1 + 2 \\ 3 = 3 \end{cases}$$

La première classe contient la permutation

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = [1]\, [2]\, [3]\,.$$

La seconde classe contient :

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = [1\ 2]\, [3]\ ,\quad c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = [2\ 3]\, [1]\ ,\quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = [1\ 3]\, [2]\,,$$

La troisième classe contient :

$$d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = [1\,2\,3]\ ,\quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = [1\,3\,2]\ .$$

FORMULE DE CAUCHY. Proposons-nous de chercher le nombre de permutations qui appartiennent à la même classe de conjuguées ; plus précisément, cherchons combien de permutations comportent :

λ_1 cycles de longueur 1
λ_2 cycles de longueur 2
.....
λ_k cycles de longueur k .

En d'autres termes, on cherche le nombre $h(\lambda_1, \lambda_2, ..., \lambda_k)$ de permutations du *type* $1^{\lambda_1}\, 2^{\lambda_2} ...\, k^{\lambda_k}$.

Construisons toutes les permutations qui se décomposent en cycles de la façon suivante :

$$\jmath = \underbrace{[\times][\times]\ldots[\times]}_{\lambda_1}\ \underbrace{[\times\ \times][\times\ \times]\ldots[\times\ \times]}_{\lambda_2}\ \ldots\ldots\ldots\ \underbrace{[\overbrace{\times\ \times\ \times}^{k}\ \times]}_{\lambda_k}.$$

Dans ce schéma, les croix figurent n fois, et peuvent être remplacées par les symboles 1, 2, ..., n de n ! façons. Cependant, ces rangements ne correspondent pas tous à des permutations distinctes, car les λ_i cycles de longueur i peuvent être permutés entre eux sans changer la permutation f. Donc la même permutation est obtenue $\lambda_1 !\ \lambda_2 !\ ...\ \lambda_k !$ fois si tous les n ! rangements sont considérés.

Par ailleurs, un cycle de longueur i peut être écrit de i façons différentes, car on peut prendre pour lettre initiale chacun de ses i éléments. Le nombre de permutations distinctes du type $1^{\lambda_1}\, 2^{\lambda_2} ...\, k^{\lambda_k}$ est donc finalement :

$$\boxed{h(\lambda_1, \lambda_2, ..., \lambda_k) = \frac{n!}{1^{\lambda_1}.\lambda_1 !\ 2^{\lambda_2}.\lambda_2 !\ \ldots\ k^{\lambda_k}.\lambda_k !}}\quad \text{(Formule de Cauchy)}.$$

Par exemple, pour $n = 3$, le nombre de permutations du type 1.2 est

$$h(1, 1, 0) = \frac{3!}{1.1!.2.1!} = 3\ .$$

Ainsi qu'on l'avait déjà vérifié plus haut, ce sont les permutations :

$$a = [1\,2]\,[3]\ ,\qquad b = [1\,3]\,[2]\ ,\qquad c = [3\,2]\,[1]\ .$$

§ 3. *Orbites d'un groupe de permutations G*

Nous allons ici généraliser la notion de cycle d'une permutation agissant sur un ensemble fini X de cardinalité n. Si $G \subseteq S_n$ est un groupe de permutations, et $x, y \in X$, on pose :

$$x \equiv y \qquad (G)$$

si il existe un $g \in G$ tel que $y = g(x)$.

On dira alors que « x est équivalent à y avec G ».

Cette relation $\equiv$ est une équivalence car

1° réflexive : $x \equiv x$, car $x = e(x)$;

2° symétrique : $x \equiv y \Rightarrow y = g(x) \Rightarrow x = g^{-1}(y) \Rightarrow y \equiv x$;

3° transitive :

$$\left.\begin{matrix} x \equiv y \\ y \equiv z \end{matrix}\right\} \Rightarrow \left.\begin{matrix} y = g(x) \\ z = g'(y) \end{matrix}\right\} \Rightarrow z = g'.g(x) \Rightarrow x \equiv z .$$

Les classes de cette équivalence sont les *orbites* du groupe G. Si l'on prend pour G le sous-groupe $\{ e, f, f^2, f^3, \ldots \}$ engendré par une permutation f, les orbites du groupe G sont les cycles de f ; pour cette raison, les orbites sont une généralisation de la notion de cycle. *Nous nous proposons maintenant de chercher le nombre d'orbites d'un groupe G.*

Pour tout $k \in X$, on dénote par

$$G_k = \{ g \mid g \in G, g(k) = k \}$$

l'ensemble des permutations de G qui laissent fixe l'élément k. *G_k est un sous-groupe de G*, car

$$f, g \in G_k \Rightarrow f.g(k) = f(k) = k \Rightarrow f.g \in G_k$$

(on applique ici le théorème 1, § 1 pour en conclure que $G_k \subseteq G$).

THÉORÈME 1. *Si O_k est l'orbite de G qui contient le point k, et si G_k est le sous-groupe de G qui laisse k invariant, on a* :

$$| G_k | \times | O_k | = | G | .$$

Considérons l'ensemble quotient G/G_k ; on sait (théorème 3, § 1) que :

$$| G/G_k | = \frac{| G |}{| G_k |} .$$

Il s'agit de montrer que ce nombre est égal à $| O_k |$, et pour cela, cherchons une application de O_k dans G/G_k qui soit bijective.

Remarquons au préalable que :

$$\left.\begin{array}{l} k = g(i) = h(i) \\ g, h \in G \end{array}\right\} \Rightarrow h.g^{-1}(k) = k \Leftrightarrow h.g^{-1} \in G_k \Leftrightarrow h \in G_k.g$$
$$\Leftrightarrow G_k.g = G_k.h$$

(en vertu du théorème 3, § 1).

A tout point $i \in O_k$, on fera correspondre une permutation $g_i \in G$ telle que $g_i(i) = k$ (elle existe toujours d'après la définition de l'orbite), et la classe $G_k.g_i \in G/G_k$.

On définit ainsi une application de O_k dans G/G_k et cette application est :

1° injective (en vertu du calcul ci-dessus) ;

2° surjective, car tout $G_k.g$ est l'image de $g^{-1}(k) \in O_k$.

On a donc bien une application bijective, d'où

$$| O_k | = | G/G_k | .$$

Exemple. Considérons le cas $n = 5$, et considérons le groupe $G \subseteq S_5$ engendré par la permutation $a = [1\ 2\ 3]\ [4\ 5]$. Les éléments de G sont :

$a = [1\ 2\ 3]\ [4\ 5]$
$a^2 = [1\ 3\ 2]\ [4]\ [5]$
$a^3 = [1]\ [2]\ [3]\ [4\ 5]$
$a^4 = [1\ 2\ 3]\ [4]\ [5]$
$a^5 = [1\ 3\ 2]\ [4\ 5]$
$a^6 = [1]\ [2]\ [3]\ [4]\ [5] = e$.

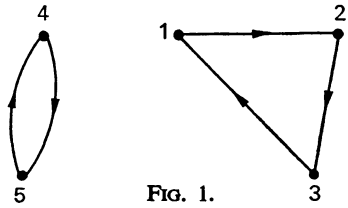


FIG. 1.

Les orbites sont ici :

$$O = \{ 1\,2\,3 \} \quad \text{et} \quad O' = \{ 4\,5 \} .$$

On a

$$O_1 = \{ 1, 2, 3 \}$$
$$G_1 = \{ a^3, a^6 \}$$
$$G = \{ a, a^2, a^3, a^4, a^5, a^6 \} .$$

On vérifie bien la relation :

$$| G_1 | \times | O_1 | = 3 \times 2 = 6 = | G | .$$

THÉORÈME 2 (Burnside). *Si $\lambda_1(g)$ est le nombre de points fixes de la permutation g (c'est-à-dire le nombre de cycles de longueur 1), le nombre d'orbites d'un groupe $G \subseteq S_n$ est :*

$$| \mathscr{C}_G | = \frac{1}{| G |} \sum_{g \in G} \lambda_1(g) .$$

En effet, en énumérant de deux manières différentes, les couples (g, k) avec $g(k) = k$, $g \in G$, $k \in X$, on a :

$$\sum_{g \in G} \lambda_1(g) = \sum_{k \in X} | G_k | = \sum_{O \in \mathscr{C}_G} \sum_{k \in O} | G_k | .$$

Si deux points j et k appartiennent à la même orbite O, on a en vertu du théorème 1 :

$$| G_j | = \frac{| G |}{| O |} = | G_k | .$$

L'égalité ci-dessus peut donc s'écrire :

$$\sum_{g \in G} \lambda_1(g) = \sum_{O \in \mathscr{C}_G} | O | \cdot \frac{| G |}{| O |} = | G | \times | \mathscr{C}_G | .$$

D'où la formule.

Ce théorème est de grande importance dans les problèmes de dénombrement, comme on le verra au chapitre suivant.

Exemple. Avec l'exemple précédent : on retrouve bien qu'il y a deux orbites, car

$$\begin{aligned} \lambda_1(a) &= 0 \\ \lambda_1(a^2) &= 2 \\ \lambda_1(a^3) &= 3 \\ \lambda_1(a^4) &= 2 \\ \lambda_1(a^5) &= 0 \\ \lambda_1(a^6) &= 5 \end{aligned}$$

$$| \mathscr{C}_G | = \tfrac{1}{6}(2 + 3 + 2 + 5) = 2 .$$

§ 4. *Parité d'une permutation*

Considérons une permutation quelconque, soit par exemple

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = 4\,5\,1\,2\,3 .$$

On dira que dans g, le symbole 1 *présente deux inversions*, car il y a deux nombres, 4 et 5, qui sont placés *avant* lui, et qui sont plus *grands* que lui. De même,

2 présente deux inversions : 4 et 5,
3 présente deux inversions : 4 et 5,
4 présente zéro inversion.
5 présente zéro inversion,

Le nombre total d'inversions de g est donc :

$$I(g) = 2 + 2 + 2 = 6 .$$

On appelle *signature* de la permutation g le nombre

$$p(g) = (-1)^{I(g)} .$$

Si $p(g) = +1$, on dit que la permutation g est *paire* ; si $p(g) = -1$ elle est *impaire.*

Une permutation qui se réduit à un cycle de longueur 2, donc de la forme $t = [i, j]$, est appelée une *transposition.*

Si $g = 4\,5\,1\,2\,3$, et si $t = [2, 3]$, on a :

$$g.t = \begin{pmatrix} 1&2&3&4&5 \\ 4&5&1&2&3 \end{pmatrix} \begin{pmatrix} 1&2&3&4&5 \\ 1&3&2&4&5 \end{pmatrix} = \begin{pmatrix} 1&2&3&4&5 \\ 4&1&5&2&3 \end{pmatrix} = 4\,1\,5\,2\,3 .$$

La suite 4 5 1 2 3 est devenue la suite 4 1 5 2 3 : les deuxième et troisième termes ont été « transposés », les autres termes de la suite restant inchangés.

On remarquera que *l'inverse d'une transposition t est égal à t.*

On se propose maintenant de chercher le nombre minimum de transpositions de la forme $[i, i + 1]$, nécessaires pour ramener une suite $k_1, k_2, ..., k_n$ à la suite 1, 2, ..., n. Par exemple, on a :

$$4\,5\,1\,2\,3 \xrightarrow{[2\ 3]} 4\,1\,5\,2\,3 \xrightarrow{[1\ 2]} 1\,4\,5\,2\,3 \xrightarrow{[3\ 4]} 1\,4\,2\,5\,3 \xrightarrow{[2\ 3]} 1\,2\,4\,5\,3$$

$$\xrightarrow{[4\ 5]} 1\,2\,4\,3\,5 \xrightarrow{[3\ 4]} 1\,2\,3\,4\,5$$

Ici, il a fallu 6 transpositions de la forme $[i, i + 1]$. Le résultat fondamental est le suivant :

THÉORÈME 1. *Le nombre minimum de transpositions de la forme* $[i, i + 1]$ *nécessaires pour ramener la suite* $g = k_1 k_2 ... k_n$ *à* $1\,2 ... n$, *est égal au nombre* $I(g)$ *d'inversions qu'elle comporte. En outre, si après q transpositions de la forme* $[i, i + 1]$, *on a ramené* $k_1, k_2, ..., k_n$, *à* 1, 2, ..., n, *alors q a nécessairement la parité de* $I(g)$.

1° Il s'agit d'abord de montrer qu'on peut toujours ramener la suite

$$k_1 k_2 ... k_n$$

à $1\,2 ... n$ par $I(g)$ transpositions. En effet, on peut amener le 1 à la première place par des échanges de deux termes consécutifs en nombre égal au nombre d'inversions que présente le 1 ; ensuite, on peut amener le 2 à la deuxième place par des échanges de deux termes consécutifs en nombre égal au nombre d'inversions que présente le 2 ; puis le 3, etc.

Chaque fois, I diminue d'une unité, comme à la fin on a $I = 0$, on a bien effectué $I(g)$ transpositions.

2° Si l'on effectue la transposition $[i, i+1]$ sur la suite $g = k_1\, k_2 \ldots k_n$, on obtient la suite $g' = k_1\, k_2 \ldots k_{i-1}\, k_{i+1}\, k_i\, k_{i+2} \ldots k_n$, avec :

$$I(g') = I(g) + 1 \quad \text{si} \quad k_i < k_{i+1}\,,$$
$$= I(g) - 1 \quad \text{si} \quad k_i > k_{i+1}\,.$$

Ceci montre que l'on ne peut jamais opérer avec moins de $I(g)$ transpositions de la forme $[i, i+1]$. Par ailleurs, si l'on peut opérer avec q transpositions de cette forme, on aura changé q fois la parité de I, pour obtenir finalement $I = 0$, donc q et $I(g)$ ont la même parité.

COROLLAIRE. *Le groupe S_n est engendré par les $n-1$ transpositions* $[1\,2]$ $[2\,3] \ldots [n-1\,n]$. *Si une permutation g peut s'écrire comme le produit de q de ces transpositions, q et $I(g)$ ont la même parité.*

En effet, dire que l'on peut ramener la suite $k_1, k_2, \ldots, k_n$ à $1, 2, \ldots, n$ par les transpositions $t_1, t_2, \ldots, t_q$, c'est dire que la permutation :

$$g = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

vérifie :

$$g.t_1.t_2.t_3.\ldots.t_q = e$$

ou

$$g = (t_1\, t_2 \ldots t_q)^{-1} = t_q^{-1}.t_{q-1}^{-1}.\ldots.t_1^{-1} = t_q.t_{q-1}.\ldots.t_1\,.$$

THÉORÈME 2. *Si $p(g) = (-1)^{I(g)}$ désigne la signature d'une permutation g, on a :*

$$p(g.g') = p(g) \times p(g')\,.$$

(*En d'autres termes, $p(g)$ est un homomorphisme du groupe de permutations S_n dans le groupe multiplicatif* $\{+1, -1\}$.)

En effet, décomposons les permutations g et g' en produits de transpositions canoniques, comme indiqué ci-dessus ; on a donc :

$$g.g' = (t_1.t_2.\ldots.t_{I(g)}).(t'_1.t'_2.\ldots.t'_{I(g')})\,.$$

C'est un produit de $I(g) + I(g')$ transpositions canoniques, donc, d'après le corollaire, $I(g) + I(g')$ a la parité de $I(g.g')$.

D'où

$$(-1)^{I(g.g')} = (-1)^{I(g)} \cdot (-1)^{I(g')}\,.$$

COROLLAIRE 1. *Si g peut s'exprimer comme le produit de q transpositions alors q a la parité de $I(g)$.*

1° *Montrons que une transposition quelconque $t = [i, j]$ est une permutation impaire.*

Partant de la suite $1, 2, ..., i-1, j, i+1, ..., j-1, i, j+1, ..., n$, on peut amener i à la i-ième place en faisant successivement les transpositions $[j-1, j]$, $[j-2, j-1]$ ... $[i, i+1]$, et il y en a exactement $j - i$.

j se trouve alors à la place $(i+1)$, et pour l'amener à la place j, il faut de même $j - (i+1)$ transpositions de la forme $[k, k+1]$. D'où un total de $2(j-i) - 1$ transpositions de la forme $[k, k+1]$. Donc $p(t) = -1$.

2° Soit $g = t_1 . t_2 ..... t_q$, où $t_1, t_2, ..., t_q$ sont des transpositions quelconques.

D'après le théorème 2, on a :

$$(-1)^{I(g)} = p(g) = p(t_1) \times p(t_2) \times \cdots \times p(t_q) = (-1)^q .$$

Donc q a la parité de $I(g)$.

COROLLAIRE 2. *Dans un groupe de permutations $G \subseteq S_n$, ou bien toutes les permutations sont paires, ou bien il y a autant de permutations paires que de permutations impaires.*

Supposons qu'il existe dans G une permutation impaire h ; donc $p(h) = -1$; l'application $g \to hg$ étant une bijection de G dans lui-même, on a

$$\sum_{g \in G} p(g) = \sum_{g \in G} p(hg) = \sum_{g \in G} p(h)\, p(g) = - \sum_{g \in G} p(g) .$$

Donc

$$\sum_{g \in G} p(g) = 0 .$$

Les permutations g avec $p(g) = +1$ sont aussi nombreuses que les permutations avec $p(g) = -1$.

COROLLAIRE 3. *Si g est une permutation de type $1^{\lambda_1} 2^{\lambda_2} ... n^{\lambda_n}$, sa parité est celle de $\lambda_2 + \lambda_4 + \lambda_6 + \cdots$; en d'autres termes la parité d'une permutation est celle du nombre total de cycles pairs qu'elle comporte.*

1° Nous allons montrer qu'un cycle de m éléments peut être décomposé en produit de $m - 1$ transpositions.

Considérons la permutation cyclique

$$g = \begin{pmatrix} k_1 & k_2 & \dots & k_m \\ k_2 & k_3 & \dots & k_1 \end{pmatrix}.$$

On peut aussi l'écrire :

$$g = [k_1\ k_2].[k_2\ k_3]. \ldots .[k_{m-1}\ k_m],$$

qui est un produit de $m - 1$ transpositions.

2° Si g est du type $1^{\lambda_1}\, 2^{\lambda_2} \ldots n^{\lambda_n}$, on peut alors l'écrire comme un produit de $\lambda_2 + 2\lambda_3 + 3\lambda_4 + \cdots$ transpositions ; donc d'après le corollaire 1, g a la parité de $\lambda_2 + \lambda_4 + \lambda_6 + \cdots$.

COROLLAIRE 4. *L'ensemble des permutations paires*

$$A_n = \{\, g \mid g \in S_n, p(g) = +1 \,\}$$

est un sous-groupe normal de S_n, appelé le « groupe alterné » ; il contient $\frac{1}{2} n\,!$ permutations.

D'une façon générale, si $\bar{g} = p(g)$ est un homomorphisme d'un groupe G dans un groupe $\overline{G}$, montrons que l'ensemble

$$K = \{\, g \mid g \in G, p(g) = \bar{e} \,\}$$

(aussi appelé le noyau de l'homomorphisme p) est toujours un sous-groupe normal de G.

1° K est un sous-groupe, car

$$g, g' \in K \Rightarrow p(g) = p(g') = \bar{e} \Rightarrow p(g.g') = p(g).p(g') = \bar{e}$$

$$\Rightarrow g.g' \in K\,.$$

2° Ce sous-groupe est normal de G, car

$$x \in Kg \Rightarrow \left.\begin{array}{r} x = kg \\ p(k) = \bar{e} \end{array}\right\} \Rightarrow p(x) = p(g)$$

$$\Rightarrow x = gh \Rightarrow x \in gK$$
$$p(h) = \bar{e}\,.$$

Comme on aurait de même les implications inverses, on a $gK = Kg$, et K est bien un sous-groupe, normal de G. D'où l'énoncé en prenant pour G le groupe de permutations S_n et pour $\overline{G}$ le groupe multiplicatif $\{ +1, -1 \}$.

Le nombre d'éléments de A_n est, d'après le corollaire 2,

$$|\, A_n \,| = \tfrac{1}{2} |\, S_n \,| = \tfrac{1}{2} n\,!\,.$$

THÉORÈME 3. *Le groupe alterné A_n est engendré par les $n - 2$ permutations circulaires*

$$t_3 = [1\ 2\ 3],\ t_4 = [1\ 2\ 4],\ \ldots,\ t_n = [1\ 2\ n]\,.$$

En effet, le groupe S_n est engendré par les transpositions [1 2], [1 3], ..., [1 n], car,

$$[1\,j].[1\,i].[1\,j] = [i\,j]\,.$$

Soit $g \in A_n$; elle peut se décomposer comme un produit d'un nombre pair de transpositions de la forme $[i\,i+1]$ donc comme un produit d'un nombre pair de transpositions de la forme $[1\,j]$.

Or, on a

$$[1\,j].[1\,i] = [1\,i\,j]\,.$$

Donc A_n est engendré par les permutations circulaires $[1\,i\,j]$. On peut aussi vérifier :

$$[1\,i\,j] = [1\,2\,j].[1\,2\,j].[1\,2\,i].[1\,2\,j]\,.$$

Donc A_n est engendré par les permutations circulaires $[1\,2\,i]$.

LEMME 1. *Si H est un sous-groupe normal de A_n (avec $n > 3$), et si H contient une permutation circulaire de trois éléments, alors $H = A_n$.*

Soit $h = [1\,2\,3] \in H$; comme H est normal dans A_n, il contient la permutation

$$g[1\,2\,3]\,g^{-1} \qquad (g \in A_n)\,.$$

En particulier, en prenant $g = [3\,2\,k]$, $k > 3$, le groupe H contient :

$$[3\,2\,k].[1\,2\,3].[k\,2\,3] = [1\,k\,2]\,.$$

Donc H contient également la permutation

$$[1\,k\,2].[1\,k\,2] = [1\,2\,k]\,.$$

Comme d'après le théorème 3, les permutations de la forme $[1\,2\,k]$ engendrent A_n, on a bien $H = A_n$.

LEMME 2. *Si H est un sous-groupe normal de A_n (avec $n > 3$), et si $h \in H$ admet un cycle de longueur > 3, alors $H = A_n$.*

Soit $h = a.b.c. \ldots$ la décomposition de h en cycles disjoints, et supposons qu'un de ces cycles soit de longueur > 3, soit par exemple :

$$a = [1\,2 \ldots m], \qquad m > 3\,.$$

Comme $g = [1\,2\,3] \in A_n$, et comme H est normal dans A_n, on a

$$h_1 = ghg^{-1} = (gag^{-1})\,bcd \ldots \in H\,,$$

Donc H contient aussi la permutation

$$\begin{aligned} h^{-1} h_1 &= (\dots c^{-1} b^{-1} a^{-1})(gag^{-1})\, bc \dots \\ &= a^{-1} gag^{-1}(\dots c^{-1} b^{-1})(bc \dots) \\ &= a^{-1} gag^{-1} = [m \dots 3\ 2\ 1]\,[1\ 2\ 3]\,[1\ 2\ 3 \dots m]\,[3\ 2\ 1] = [1\ 3\ m]\,. \end{aligned}$$

Donc, d'après le lemme 1, on a $H = A_n$.

THÉORÈME DE GALOIS. *Si $n > 4$, les seuls sous-groupes normaux de A_n sont A_n et $\{ e \}$.*

Soit $n > 4$, et H un sous-groupe normal de A_n différent de A_n et de $\{ e \}$.
Si $h \in H$, la permutation h se décompose en cycles a, b, c, ... de longueur 2 et en cycles a', b', c', ... de longueur 3 (d'après le lemme 2) ; ces cycles sont disjoints, donc les permutations correspondantes commutent.

1° Si h contient deux cycles de longueur 3, on peut supposer

$$h = [1\ 2\ 3].[4\ 5\ 6].h'\,.$$

Comme $g = [2\ 3\ 4] \in A_n$, le groupe H contient la permutation :

$$h_1 = ghg^{-1} = [2\ 3\ 4]\,[1\ 2\ 3]\,[4\ 5\ 6]\,[4\ 3\ 2]\,h' = [1\ 3\ 4].[2\ 5\ 6]\,h'\,.$$

H contient aussi la permutation

$$\begin{aligned} h^{-1} h_1 &= [3\ 2\ 1]\,[6\ 5\ 4]\,h'^{-1}\,[1\ 3\ 4]\,[2\ 5\ 6]\,h' \\ &= [3\ 2\ 1]\,[6\ 5\ 4]\,[1\ 3\ 4]\,[2\ 5\ 6] = [1\ 2\ 4\ 3\ 6]\,. \end{aligned}$$

Donc d'après le lemme 2, $H = A_n$, ce qui contredit notre hypothèse.

2° Si h contient un seul cycle de longueur 3, on peut écrire

$$h = [1\ 2\ 3]\,h'\,,$$

où h' ne contient que ces cycles de longueur 1 ou 2.
Donc H contient

$$h^2 = [1\ 2\ 3]\,[1\ 2\ 3]\,(h')^2 = [1\ 3\ 2]\,.$$

Donc d'après le lemme 1, $H = A_n$; ce qui contredit notre hypothèse.

3° Si h ne contient pas de cycles de longueur 3, on peut écrire, comme $n > 4$

$$h = [1\ 2].[3\ 4]\,h'\,,$$

où h' ne contient que des cycles de longueur 1 ou 2.

Comme $g = [2\ 3\ 4] \in A_n$, le groupe H contient la permutation

$$h_1 = ghg^{-1} = [2\ 3\ 4]\,[1\ 2].[3\ 4]\,[4\ 3\ 2]\,h' = [1\ 3]\,[2\ 4]\,h'\,.$$

H contient aussi :

$$h_2 = h^{-1} h_1 = [2\ 1]\,[4\ 3]\,[1\ 3]\,[2\ 4] = [1\ 4]\,[2\ 3]\,.$$

Comme $[1\ 4\ 5] \in A_n$, H contient aussi

$$h_3 = [1\ 4\ 5]\,h_2[1\ 4\ 5]^{-1} = [1\ 4\ 5]\,[1\ 4]\,[2\ 3]\,[5\ 4\ 1] = [2\ 3]\,[4\ 5]\,.$$

H contient aussi

$$h_2\,h_3 = [1\ 4]\,[2\ 3]\,[2\ 3]\,[4\ 5] = [1\ 4\ 5]\,.$$

D'après le lemme 1, $H = A_n$, ce qui contredit notre hypothèse.
Le théorème est donc démontré.

Remarque.

Si $n = 2$, on a $A_n = \{ e \}$.

Si $n = 3$, on a vu (§ 1) que $A_n = \{ e, d, f \}$ et ne contient pas de sous-groupes normaux autres que A_n et $\{ e \}$ (exemple, § 1).

Si $n = 4$, cherchons s'il existe un sous-groupe normal H de A_n, autre que A_n et $\{ e \}$.

Si $h \in H$, la permutation h est paire, donc d'après le corollaire 3 du théorème 2, elle comporte 0 ou 2 cycles pairs.

Le type 1^4 donne la permutation e.

Le type 1.3 est impossible, d'après le lemme 1. Donc H contient une permutation du type 2^2, soit par exemple

$$h = [1\ 2]\,[3\ 4]$$

H contient aussi

$$[1\ 2\ 3]\,h[1\ 2\ 3]^{-1} = [1\ 2\ 3]\,[1\ 2]\,[3\ 4]\,[3\ 2\ 1] = [1\ 4]\,[2\ 3]$$

$$[1\ 3\ 4]\,h[1\ 3\ 4]^{-1} = [1\ 3\ 4]\,[1\ 2]\,[3\ 4]\,[4\ 3\ 1] = [1\ 4]\,[2\ 3]$$

$$[2\ 3\ 4]\,h[2\ 3\ 4]^{-1} = [2\ 3\ 4]\,[1\ 2]\,[3\ 4]\,[4\ 3\ 2] = [1\ 3]\,[2\ 4] \text{ etc.}$$

Finalement, on trouve un sous-groupe normal H, composé de

$$e,\ [1\ 2]\,[3\ 4],\ [1\ 3]\,[2\ 4],\ [1\ 4]\,[2\ 3]$$

Ce groupe H est parfois appelé *le groupe V*, de l'allemand : « Vierer Gruppe ».

Il est à noter que le théorème de Galois a une application célèbre (due à Evariste Galois) : il permet de montrer que les racines d'une équation algébrique de degré $n > 4$ ne peuvent pas être explicitées par une formule algébrique avec seulement des radicaux.

Application : Le Permutoèdre.

Construisons un graphe en représentant par des points les n ! permutations de $X = \{1, 2, ..., n\}$ et en joignant deux permutations f et g si $f = tg$ pour une transposition t. Ce graphe peut être représenté par un polyèdre convexe (Fig. 2), que G. GUILBAUD et P. ROSENSTIEHL [1] ont proposé d'appeler « permutoèdre ».

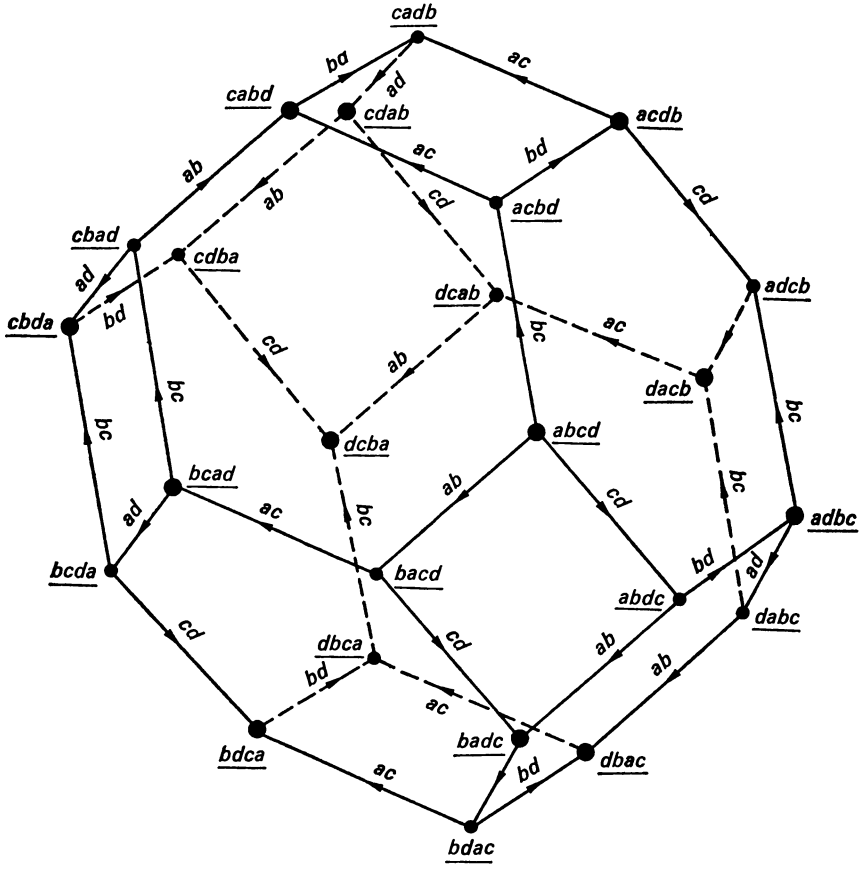


FIG. 2. — *Représentation du graphe des permutations de a, b, c, d par un polyèdre convexe* (« *permutoèdre* »). (Chaque transposition est représentée par un vecteur distinct, leur ensemble constituant les arêtes du permutoèdre).

Si deux points $f = x_1\, x_2 \ldots x_i \ldots x_j \ldots x_n$ et $g = x_1\, x_2 \ldots x_j \ldots x_i \ldots x_n$ sont adjacents, on tracera une flèche allant de f vers g si $x_i < x_j$, ou de g vers f si $x_j < x_i$. Nous nous proposons de démontrer, suivant P. ROSENSTIEHL [2], que cette construction définit un treillis.

Si $f = x_1\, x_2 \ldots x_n$, désignons par $E(f)$ l'ensemble des couples $x_i\, x_j$ ne pré-

sentant pas d'inversion dans f, il y en a $\frac{n(n-1)}{2} - I(f)$; et par $E^*(f)$ l'ensemble des couples qui présentent une inversion, il y en a $I(f)$.

$$E(f) = \{ x_i x_j / i < j, x_i < x_j \},$$

$$E^*(f) = \{ x_i x_j / i < j, x_i > x_j \}.$$

Donnons-nous un ensemble E de couples xy, avec $x < y$, et dénotons par E^* l'ensemble des couples xy avec $x > y$ et $yx \notin E$. Le graphe orienté $(X, E \cup E^*)$ est construit de la façon suivante : les points représentent les éléments de $X = \{ 1, 2, ..., n \}$, et l'on trace un arc (avec une flèche) allant de x à y si $xy \in E \cup E^*$. Ce graphe est *complet*, c'est-à-dire que pour deux points x et y quelconques $(x < y)$, il existe soit un arc de x vers y (si $xy \in E$), soit un arc de y vers x (si $yx \in E^*$).

LEMME. *Si un graphe complet n'admet pas de circuits, il admet un chemin $a_1, a_2, ..., a_n$ passant une fois et une fois seulement par chaque sommet du graphe, et ce chemin est unique.*

En effet, il existe au moins un sommet qui n'est l'extrémité terminale d'aucune flèche, car sans cela on pourrait parcourir le graphe indéfiniment en remontant les flèches, ce qui est absurde car le graphe n'a pas de circuits. Soit a_1 ce sommet ; un tel sommet est unique, car s'il y en avait deux a_1 et a_1', ils seraient joints dans au moins une direction, ce qui est absurde.

De même, il existe, dans le sous-graphe engendré par $X - \{ a_1 \}$, un sommet a_2 (unique) qui n'est l'extrémité terminale d'aucune flèche, et $a_1 a_2$ est un arc.

De proche en proche, on trouve le chemin unique $a_1, a_2, a_3, ...$

PROPOSITION 1. *Si pour un ensemble E de couples xy avec $x < y$, le graphe $(X, E \cup E^*)$ n'admet pas de circuits, il existe exactement une permutation f avec $E(f) = E$; si le graphe admet un circuit, il n'existe aucune permutation f avec $E(f) = E$.*

Si le graphe possède un circuit, il n'existe évidemment pas de permutation f avec $E(f) = E$.

Si le graphe n'admet pas de circuit, il existe d'après le lemme un chemin unique $a_1, a_2, ..., a_n$, et l'on a nécessairement

$$f = a_1 a_2 ... a_n .$$

On a bien $E(f) = E$.

PROPOSITION 2. *Posons $f \geqslant g$ si $E(f) \supset E(g)$; la relation $\geqslant$ est une relation d'ordre.*

En effet, on a d'après la proposition 1 :

$$f \geqslant f$$

$$\left.\begin{matrix} f \geqslant g \\ g \geqslant f \end{matrix}\right\} \Rightarrow E(f) = E(g) \quad \Rightarrow \quad f = g$$

$$\left.\begin{matrix} f \geqslant g \\ g \geqslant h \end{matrix}\right\} \Rightarrow f \geqslant h\,.$$

PROPOSITION 3. *Désignons par $\overline{A}$ la fermeture transitive de A, c'est-à-dire l'ensemble des couples xy liés par un chemin allant de x à y dans le graphe (X, A). Si f et g sont deux permutations, il existe une permutation unique, notée $f \vee g$, telle que*

$$E(f \vee g) = \overline{E(f) \cup E(g)}$$

$f \vee g$ est le plus petit majorant de f et de g.

Il s'agit de montrer, d'après la proposition 1, que le graphe ayant pour arcs les couples de $E = \overline{E(f) \cup E(g)}$ et de E^*, est sans circuits.

Ce graphe, étant complet et antisymétrique, s'il admettait un circuit, aurait un circuit abc de longueur 3.

Si l'on suppose $a < b < c$, on a

$$ab,\ bc \in E\,;\ ca \in E^*\,.$$

Ce qui est absurde, car E étant transitif, on a $ac \in E$.

Si l'on suppose que le circuit est acb, avec $a < b < c$, on a

$$ac \in E\,;\ cb,\ ba \in E^*\,.$$

Comme $bc,\ ab \notin E(f) \cup E(g)$, on a

$$cb,\ ba \in E^*(f) \cap E^*(g)\,.$$

Comme $E^*(f)$ est transitif, on a $ca \in E^*(f) \cap E^*(g)$, donc

$$ac \notin E(f) \cup E(g)\,.$$

Il existe donc un point $x \neq c$, avec

$$ax \in E(f), \qquad xc \in E(g), \qquad a < x < c\,.$$

Or

$$b < x \Rightarrow \left\{\begin{matrix} b < x \\ bx \in E(f) \cup E^*(f) \end{matrix}\right. \quad \Rightarrow \quad bx \in E(f) \Rightarrow bc \in E : \text{absurde}$$

$$b > x \Rightarrow \left\{\begin{matrix} b > x \\ xb \in E(g) \cup E^*(g) \end{matrix}\right. \quad \Rightarrow \quad xb \in E(g) \Rightarrow ab \in E : \text{absurde}\,.$$

PROPOSITION 4. *Il existe une permutation unique, notée* $f \wedge g$, *telle que*

$$E^*(f \wedge g) = \overline{E^*(f) \cup E^*(g)}$$

$f \wedge g$ *est le plus grand majorant de* f *et de* g.

(Ceci se déduit de la proposition 3 par symétrie, en inversant l'ordre sur X).

On en déduit que le permutoèdre est bien un treillis.

§ 5. *Problèmes de décompositions*

Considérons une permutation f sur un ensemble X d'objets, que l'on dénotera par des lettres $x_1, x_2, \ldots, x_n$.

On peut lui faire correspondre un graphe G_f, en représentant les x_i par des points (ou *sommets*), et en traçant les *arcs* $(x_i, f(x_i))$; ce graphe sera composé de *circuits* disjoints, qui partitionnent X. Considérons d'autre part un ensemble $T = \{ t_1, t_2, \ldots, t_k \}$ de transpositions ; on peut lui faire correspondre un graphe (X, T), dont les sommets sont les x_i, et les *arêtes* $[x_i\ x_j]$ les transpositions de l'ensemble T.

Exemple. $X = \{ a, b, c, d \}$.

T est constitué des transpositions $t_1 = [ab]$, $t_2 = [bc]$, $t_3 = [bd]$

$$f = t_1\, t_2\, t_3 = [ab]\,[bc]\,[bd] = \begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

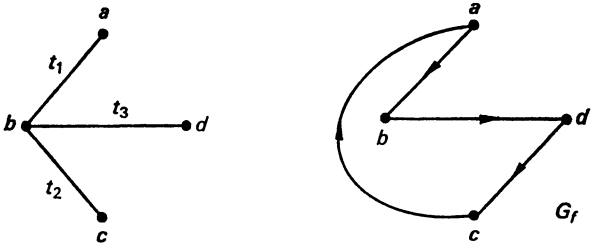


FIG. 3.

$$g = t_2\, t_3\, t_1 = [bc]\,[bd]\,[ab] = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$$

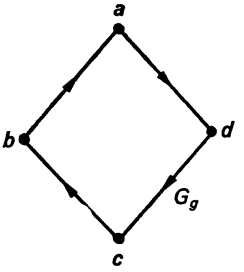


FIG. 4.

$$gt_1 = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix} [ab] = \begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}$$

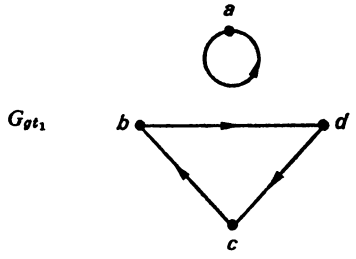


FIG. 5.

$$t_1 g = [ab] \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}.$$

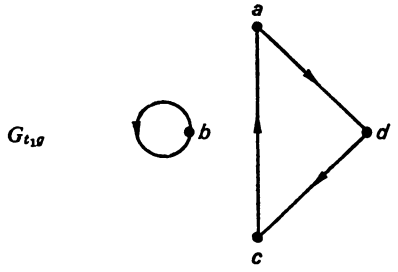


FIG. 6.

THÉORÈME 1. *Un ensemble T de $n-1$ transpositions engendre le groupe symétrique S_n si et seulement si (X, T) est un arbre.*

1° Si (X, T) est un arbre, toute transposition $[ab]$ est un produit de transpositions de T. En effet, d'après la propriété (6) du théorème 1 (Chap. 3, § 5), il existe dans (X, T) une chaîne $[a\, x_1]$, $[x_1\, x_2]$, ..., $[x_k\, b]$ reliant a et b, et

$$[a\ b] = [x_k\ b]\ [x_{k-1}\ x_k] \ldots [x_2\ x_3]\ [x_1\ x_2]\ [a_1\ x_1]\ [x_1\ x_2] \ldots [x_{k-1}\ x_k]\ [x_k\ b].$$

Comme le groupe symétrique S_n est engendré par les transpositions, il est donc bien engendré par T.

2° Si (X, T) n'est pas un arbre, il contient au moins deux ensembles X_1 et X_2 disjoints et non reliés par une arête (théorème 1, chap. 3, § 5). Si $a \in X_1$, $b \in X_2$, la transposition $[a\ b]$ ne peut donc pas être un produit d'éléments de T.

LEMME. *Soit f une permutation sur X, et $g = f.[ab]$ le produit de f et d'une transposition $[a\ b]$.*

Le graphe G_g se déduit du graphe G_f en remplaçant les arcs $(a, f(a))$ et $(b, f(b))$ par les arcs $(a, f(b))$ et $(b, f(a))$.

1° *Si a et b sont sur deux cycles différents de G_f, ces deux cycles n'en forment plus qu'un dans G_g ; en outre, si $\mu_f(x, y)$ représente l'ensemble des sommets rencontrés en parcourant le chemin élémentaire de G_f allant de x à y, ($\mu_f(x, y) = \varnothing$ si x et y ne sont pas connectés), on a*

$$z \in \mu_f(x, y) \quad \Rightarrow \quad z \in \mu_g(x, y)\ .$$

2° *Si a et b sont sur le même cycle de G_f, ce cycle est décomposé en deux cycles disjoints dans G_g ; en outre,*

$$\left.\begin{array}{l} \mu_g(x, y) \neq \varnothing \\ z \in \mu_f(x, y) \end{array}\right\} \Rightarrow z \in \mu_g(x, y)\ .$$

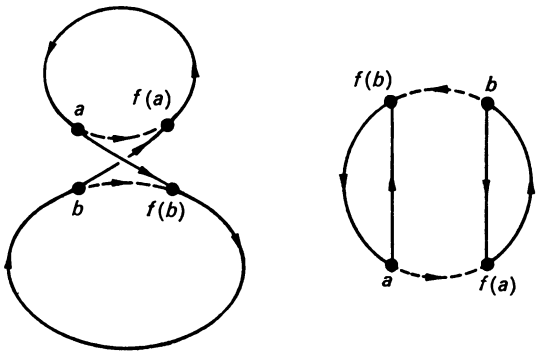


FIG. 7.

Ceci est évident ; si a et b appartiennent à deux cycles distincts, on a

$$\begin{aligned} g = f[a\ b] &= [a, fa, f^2 a, ...]\ [b, fb, f^2 b, ...]\ h[ab] \\ &= [a, fb, f^2 b, ..., b, fa, f^2 a, ...]\ h\ . \end{aligned}$$

Si a et b appartiennent au même cycle, on a

$$g = f[a\ b] = [a, fa, ..., b, fb, ...]\ h[a, b] = [a, fb, ...]\ [b, fa, ...]\ h\ .$$

THÉORÈME 2 (Dénès). *Soit $T = \{ t_1, t_2, ..., t_{n-1} \}$ un ensemble de $n - 1$ transpositions. Le produit $f = t_1\ t_2 ...\ t_{n-1}$ est une permutation circulaire de degré n (c'est-à-dire : G_f est un circuit unique), si et seulement si (X, T) est un arbre.*

1) Soit (X, T) un arbre.

Considérons les graphes des permutations :

$$g_1 = t_1\,, \quad g_2 = g_1\, t_2\,, \quad g_3 = g_2\, t_3, \ldots, g_{n-1} = f\,.$$

D'après le lemme, le nombre de composantes connexes est

$$p(G_{g_1}) = n - 1\,,$$

$$p(G_{g_2}) = p(G_{g_1}) - 1 = n - 2\,,$$

$$p(G_{g_3}) = p(G_{g_2}) - 1 = n - 3\,,$$

$$\ldots$$

$$p(G_f) = p(G_{g_{n-2}}) - 1 = 1\,.$$

G_f, étant connexe, est composé d'un circuit unique.

2) Si (X, T) n'est pas un arbre, il contient au moins deux composantes connexes X_1 et X_2 (Chap. 3, § 5). Si $a \in X_1$, $b \in X_2$, les points a et b ne seront pas sur le même circuit dans le graphe G_{g_1} ; d'après le lemme, si a et b ne sont pas sur un même circuit dans le graphe G_{g_i} ils ne seront pas davantage sur un même circuit dans le graphe $G_{g_{i+1}}$. Donc ils seront disconnectés sur le graphe G_f, donc f ne peut pas être une permutation circulaire de degré n.

COROLLAIRE ([5]). *Si f est une permutation circulaire de degré n, le nombre de façons $A(f)$ d'écrire f comme un produit de $n - 1$ transpositions est égal à n^{n-2}.*

En effet, le nombre de permutations circulaires de degré n est $(n - 1)!$, chacune pouvant s'écrire de $A(f)$ façons différentes. Le nombre de produits de $(n - 1)$ transpositions donnant une permutation circulaire de degré n est donc $A(f)\ (n - 1)!$. D'autre part, d'après le théorème précédent, c'est aussi $(n - 1)!$ fois le nombre d'arbres ayant n sommets donnés (qui est n^{n-2}, d'après la formule de Cayley, chap. 3, § 5). On a donc finalement :

$$A(f) = n^{n-2}\,.$$

Proposons-nous maintenant de chercher le nombre de permutations circulaires de degré n distinctes qui peuvent être obtenues avec les arêtes d'un arbre (X, T) donné.

Soit $\bar{g} = t_1\, t_2 \ldots t_{n-1}$ un mot formé des $n - 1$ arêtes de l'arbre (X, T), et soit $h_k(\bar{g})$ le mot formé des arêtes incidentes au sommet x_k dans l'ordre où ils apparaissent dans le mot $\bar{g}$.

Deux mots $\bar{g} = t_1\, t_2 \ldots t_{n-1}$ et $\bar{g}' = t'_1\, t'_2 \ldots t'_{n-1}$ peuvent vérifier $h_k(\bar{g}) = h_k(\bar{g}')$ pour tout k ; par exemple, si $X = \{ x_1, x_2, x_3, x_4 \}$, et si T est composé de

$t_1 = [x_1\, x_2]$, $t_2 = [x_2\, x_3]$ et $t_3 = [x_3\, x_4]$, et si $\bar{g} = t_2\, t_1\, t_3$ et $\bar{g}' = t_2\, t_3\, t_1$, on a

$$h_1(\bar{g}) = h_1(\bar{g}') = t_1\,,$$

$$h_2(\bar{g}) = h_2(\bar{g}') = t_2\, t_1\,,$$

$$h_3(\bar{g}) = h_3(\bar{g}') = t_2\, t_3\,,$$

$$h_4(\bar{g}) = h_4(\bar{g}') = t_3\,.$$

THÉORÈME 3 (M. Eden, M. P. Schützenberger). *Deux mots* $\bar{f} = t_1\, t_2 \ldots t_{n-1}$ et $\bar{g} = t'_1\, t'_2 \ldots t'_{n-1}$ *formés avec les* $n-1$ *arêtes d'un arbre* (X, T), *donnent des permutations circulaires* f *et* g *égales si et seulement si on a* :

$$h_k(\bar{f}) = h_k(\bar{g}) \qquad (k = 1, 2, \ldots, n)\,.$$

1) *Montrons que si la permutation* g *est de la forme*

$$g = g_1\, t g_2\, t'\, g_3\,, \qquad t = [x_k\, a]\,, \qquad t' = [x_k\, b]\,,$$

alors

$$x_k \in \mu_g(a, b)\,.$$

Considérons le graphe de la permutation $g_1\, t g_2$; d'après le lemme précédent, a et x_k sont sur un même circuit et b sur un autre circuit.

Donc

$$\begin{aligned} g_1\, t g_2\, t' &= [a, f(a), \ldots, x_k, f(x_k) \ldots]\, [b, f(b) \ldots]\, g' [x_k\, b] \\ &= [x_k, f(b), \ldots, b, f(x_k) \ldots a, f(a) \ldots]\, g'\,. \end{aligned}$$

Donc

$$x_k \in \mu_{g_1 t g_2 t'}(a, b)\,,$$

et d'après le lemme précédent, on a bien :

$$x_k \in \mu_g(a, b)\,.$$

2) Soient $\bar{f}$ et $\bar{g}$ deux mots pour lesquels

$$h_k(\bar{f}) \neq h_k(\bar{g})\,.$$

Montrons que les permutations circulaires correspondantes f et g sont différentes.

Il existe deux transpositions $[x_k\, a]$ et $[x_k\, b]$ qui figurent dans cet ordre dans $\bar{f}$ et dans l'ordre inverse dans $\bar{g}$. Donc, d'après 1)

$$x_k \in \mu_f(a, b) \qquad x_k \in \mu_g(b, a)$$

et par conséquent $f \neq g$.

3) Si $h_i(\bar{f}) = h_i(\bar{g})$ pour $i = 1, 2, ..., n$, montrons que $f = g$. Essayons, en échangeant deux symboles t consécutifs de $\bar{g}$ correspondant à des arêtes disjointes, de ramener le début du mot $\bar{g}$ à celui du mot $\bar{f}$ (ce qui ne modifie pas $\bar{g}$) ; à un certain moment, on ne pourra plus continuer (dans le cas contraire, on aurait démontré $f = g$). On obtient alors :

$$\bar{f} = \bar{f}_1[x_j\, x_k]\,\bar{f}_2\,,$$

$$\bar{g} = \bar{f}_1\,\bar{g}_1[x_j\, x_k]\,\bar{g}_2\,.$$

Comme dans $\bar{g}$, l'arête $[x_j\ x_k]$ ne peut pas être déplacée vers la gauche contre $\bar{f}_1$, le mot $\bar{g}_1$ contient une arête d'extrémité x_j ou x_k, soit par exemple $[x_k\, x_p]$. On a

$$\bar{f} = \bar{f}_1[x_j\, x_k]\,\bar{f}_2'[x_k x_p]\bar{f}_3'\,,$$

$$\bar{g} = \bar{f}_1\,\bar{g}_1'[x_k\, x_p]\,[x_j\, x_k]\,\bar{g}_2\,.$$

Donc $h_k(\bar{f}) \neq h_k(\bar{g})$, ce qui est contraire à l'hypothèse.

CONSÉQUENCE 1

Etant donnée une permutation circulaire f et un arbre (X, T), cherchons s'il est possible d'écrire

$$f = t_1\, t_2 ... \, t_{n-1}\,, \qquad \text{avec} \qquad t_1, t_2, ..., t_{n-1} \in T\,.$$

Par exemple, prenons

$$f = [1\,3\,8\,2\,5\,4\,6\,7]\,.$$

T est composé des arêtes

$$t_1 = [x_1\, x_3]\,, \qquad t_2 = [x_3\, x_8]\,,$$

etc., comme sur la figure 8.

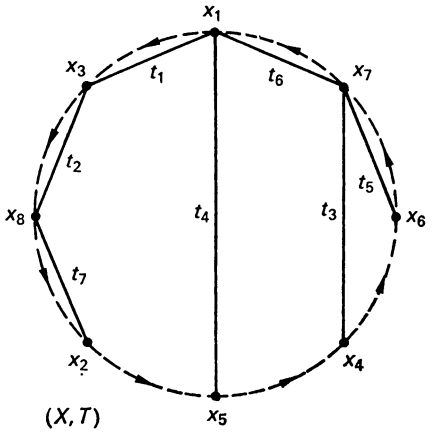


FIG. 8.

Supposons que f puisse s'écrire avec les $n - 1$ arêtes de l'arbre (X, T). On a

$$h_1(\bar{f}) = [x_1\ x_7]\ [x_1\ x_5]\ [x_1\ x_3] = t_6\ t_4\ t_1\ .$$

En effet, $[x_1\ x_7]$ et $[x_1\ x_5]$ se trouvent placés dans cet ordre, d'après le 1) du théorème 3, car

$$x_1 \in \mu_f(x_7, x_5)\ .$$

On prend donc les arêtes de T incidentes à x_1 dans l'ordre où elles se rencontrent en parcourant le circuit en sens inverse à partir de x_1. On a de même

$$h_2(\bar{f}) = t_7$$

$$h_3(\bar{f}) = t_1\ t_2$$

$$h_4(\bar{f}) = t_3$$

$$h_5(\bar{f}) = t_4$$

$$h_6(\bar{f}) = t_5$$

$$h_7(\bar{f}) = t_5\ t_3\ t_6$$

$$h_8(\bar{f}) = t_2\ t_7\ .$$

Il est toujours possible de trouver un mot $\bar{f}$ vérifiant les égalités ci-dessus (car T est un arbre et n'a pas de cycles).

On obtient ici :

$$\bar{f} = t_5\ t_3\ t_6\ t_4\ t_1\ t_2\ t_7\ .$$

Donc

$$f = [x_6\ x_7]\ [x_7\ x_4]\ [x_7\ x_1]\ [x_1\ x_5]\ [x_1\ x_3]\ [x_3\ x_8]\ [x_8\ x_2]$$

$$= \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,5\,8\,6\,4\,7\,1\,2 \end{pmatrix} = [1\,3\,8\,2\,5\,4\,6\,7]\ .$$

Donc il est possible d'écrire f avec les arêtes de l'arbre T.

CONSÉQUENCE 2

Si (X, T) est un arbre avec des degrés $d(x_i)$, $i = 1, 2, \ldots, n$, le nombre de permutations circulaires distinctes de degré n qu'on obtient comme produit de ses $n - 1$ arêtes est :

$$\prod_{i=1}^{n} d(x_i)!$$

Ce résultat montre en particulier qu'un arbre donné ne peut pas, en général, engendrer toutes les permutations circulaires de degré n, qui sont en nombre $(n - 1)$!

5

La méthode de Polyà

§ 1. *Dénombrement des schémas par rapport à un groupe de permutations des objets*

On se donne ici un ensemble d'objets $X = \{ 1, 2, ..., n \}$, un groupe G de permutations dans X, et une application φ de X dans un ensemble

$$A = \{ a_1, a_2, ..., a_m \} .$$

Pour concrétiser, on dira ici que A est un *ensemble de couleurs*, et φ une *coloration* — chaque objet i étant « coloré » avec la couleur $\varphi(i)$.

Remarquons que si $g \in G$, l'application φg est encore une coloration ; par exemple :

$$\varphi . g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ b & c & a & a & c \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & c & b & c & a \end{pmatrix} .$$

On dira que deux colorations φ_1 et φ_2 appartiennent au même *schéma* — et l'on écrira $\varphi_1 \sim \varphi_2$ — s'il existe une permutation $g \in G$ telle que $\varphi_1 g = \varphi_2$

La relation $\varphi_1 \sim \varphi_2$ est bien une équivalence ;

$\varphi \sim \varphi$, car $\varphi = \varphi e$, $e \in G$;

$\varphi_1 \sim \varphi_2 \Rightarrow \varphi_2 \sim \varphi_1$, car $\varphi_1 (g(x)) = \varphi_2(x) \Rightarrow \varphi_1(y) = \varphi_2(g^{-1}(y))$

$\varphi_1 \sim \varphi_2, \varphi_2 \sim \varphi_3 \Rightarrow \varphi_1 \sim \varphi_3$, car

$$\left.\begin{array}{l} \varphi_1(g(y)) = \varphi_2(y) \\ \varphi_2(h(x)) = \varphi_3(x) \end{array}\right\} \Rightarrow \varphi_1 gh(x) = \varphi_3(x) .$$

Cette relation d'équivalence partage l'ensemble des colorations en classes d'équivalences — ou schémas — que l'on se propose de dénombrer.

Exemple 1. *Colorations du cube.*

Considérons pour X les faces d'un cube, soit $X = \{ 1, 2, 3, 4, 5, 6 \}$, que l'on se propose de colorier avec deux couleurs : noir et blanc, soit $A = \{ n, b \}$.

Proposons-nous de chercher combien il y a de schémas de cubes colorés, deux cubes étant considérés comme équivalents si on peut les amener à coïncider par déplacement.

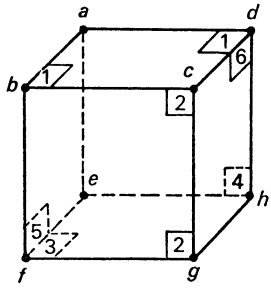


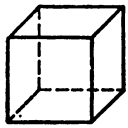
FIG. 1.

Ici, une coloration de cube est une application de X dans A ; G est le groupe de toutes les rotations de cubes :

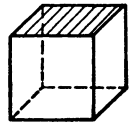
autour de l'axe	*abcd-efgh* :	[2 6 4 5] ; [2 4] [6 5] ; [2 5 4 6]
— —	*bcfg-adhe* :	[1 5 3 6] ; [1 3] [5 6] ; [1 6 3 5]
— —	*abfe-dcgh* :	[1 2 3 4] ; [1 3] [2 4] ; [1 4 3 2]
— de l'axe	*a-g* :	[1 4 5] [6 3 2] ; [1 5 4] [6 2 3]
— —	*b-h* :	[1 5 2] [6 4 3] ; [1 2 5] [6 3 4]
— —	*c-e* :	[1 2 6] [3 4 5] ; [1 6 2] [3 5 4]
— —	*d-f* :	[1 6 4] [3 5 2] ; [1 4 6] [3 2 5]
autour de l'axe	*ab-hg* :	[1 5] [6 3] [2 4]
— —	*bc-eh* :	[1 2] [4 3] [5 6]
— —	*cd-ef* :	[1 6] [3 5] [2 4]
— —	*ad-fg* :	[1 4] [2 3] [5 6]
— —	*bf-dh* :	[2 5] [6 4] [1 3]
— —	*cg-ae* :	[2 6] [5 4] [1 3]

Avec la permutation identique [1] [2] [3] [4] [5] [6], on trouve 24 permutations.

Les schémas sont au nombre de 10.

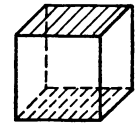


0 face noire

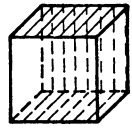


1 face noire

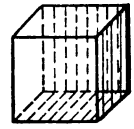
2 faces noires



2 faces noires



3 faces noires



3 faces noires etc.

Exemple 2. *Rangements d'une collection d'objets.*

Considérons un ensemble de trois objets $X = \{ 1, 2, 3 \}$, 1 étant une boule B et 2 et 3 des cubes analogues C, qu'on veut ranger dans des boîtes désignées par a, b, c. toutes distinguables.

Un rangement est une application φ de X dans $\{ a, b, c \}$. Le groupe G consiste en deux permutations : [1] [2] [3] et [1] [2 3].

On trouve 18 schémas possibles :

$BCC \mid \varnothing \mid \varnothing$;
$BC \mid C \mid \varnothing$
$BC \mid \varnothing \mid C$
$CC \mid B \mid \varnothing$
$CC \mid \varnothing \mid B$
$B \mid CC \mid \varnothing$
$B \mid C \mid C$
$B \mid \varnothing \mid CC$

$C \mid BC \mid \varnothing$
$C \mid B \mid C$
$C \mid C \mid B$
$C \mid \varnothing \mid BC$
$\varnothing \mid BCC \mid \varnothing$
$\varnothing \mid BC \mid C$
$\varnothing \mid CC \mid B$
$\varnothing \mid B \mid CC$
$\varnothing \mid C \mid BC$
$\varnothing \mid \varnothing \mid BCC$

Plus généralement, considérons une collection d'objets $X = \{ 1, 2, ..., n \}$ partitionnée par une partition $(S_1, S_2, ..., S_k)$ de type $\alpha_1 + \alpha_2 + \cdots + \alpha_k$.

Les objets d'une même classe seront considérés comme indistinguables entre eux — ou « de la même espèce ». On veut les ranger dans m boîtes distinctes $a_1, a_2, ..., a_m$. Le groupe G se compose des permutations g telles que

$$x \in S_i \Rightarrow g(x) \in S_i \qquad (i = 1, 2, \ldots k)$$

il y en a $\alpha_1 ! \alpha_2 ! \ldots \alpha_k !$

THÉORÈME 1 (Polyà). *Si $g \in G$, désignons par $\lambda_i(g)$ le nombre de cycles de longueur i de la permutation g, et appelons indicateur de cycles de G le polynôme :*

$$P(G\,;\,x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{\lambda_1(g)}\, x_2^{\lambda_2(g)} \ldots x_n^{\lambda_n(g)}\,.$$

Le nombre de schémas est égal à

$$P(G\,;\,m, m, \ldots, m)\,.$$

Par exemple, dans le cas des colorations du cube, on a

$$P(G\,;\,x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}(x_1^6 + 3\,x_1^2\,x_2^2 + 6\,x_1^2\,x_4 + 6\,x_2^3 + 8\,x_3^2)\,.$$

Le nombre de schémas du cube est donc :

$$P(G\,;\,2, 2, 2, 2, 2, 2) = 10\,.$$

Dans le cas du rangement d'une boule et de deux cubes dans trois boîtes distinguables, on a :

$$P(G\,;\,x_1, x_2, x_3) = \frac{1}{2}(x_1^3 + x_1\,x_2)\,.$$

Le nombre de schémas est donc :

$$P(G\,;\,3, 3, 3) = 18\,.$$

Démonstration.

Considérons une coloration $\varphi \in \Phi$ et une permutation $g \in S_n$; l'application $\varphi \to \bar{g}(\varphi) = \varphi g$ est une injection de Φ dans lui-même, car

$$\varphi \neq \varphi' \quad \Rightarrow \quad \varphi g \neq \varphi'\, g \quad \Rightarrow \quad \bar{g}(\varphi) \neq \bar{g}(\varphi')\,.$$

Comme Φ est fini, cette application est bijective, donc $\bar{g} \in \bar{S}$, ensemble des permutations de l'ensemble Φ.

L'application $g \to \bar{g}$, de G dans $\bar{S}$, est injective, car

$$\begin{aligned} g \neq g' &\Rightarrow g(k) \neq g'(k) \text{ pour un } k \leqslant n \\ &\Rightarrow \varphi g \neq \varphi g' \quad \text{pour une coloration } \varphi \text{ colorant différemment } g(k) \text{ et } g'(k) \\ &\Rightarrow \bar{g} \neq \bar{g}'\,. \end{aligned}$$

Donc $\bar{G} = \{\, \bar{g} \mid g \in G \,\}$ a la même cardinalité que G. D'autre part, $\bar{G}$ est un sous-groupe de $\bar{S}$, car $g, h \in \bar{G}$ implique

$$\bar{g}.\bar{h}(\varphi) = \bar{g}(\varphi h) = \varphi(hg) = (\overline{hg})\,\varphi\,,$$

donc $\bar{g}.\bar{h} \in \bar{G}$.

Deux colorations φ_1 et φ_2 sont équivalentes si $\varphi_1 = \bar{g}(\varphi_2)$ pour un $\bar{g} \in \bar{G}$, donc si elles appartiennent à une même orbite du groupe $\bar{G}$ (Cf. Chap. 4, § 3) ; le nombre de schémas est donc le nombre d'orbites de $\bar{G}$, c'est-à-dire, d'après le théorème 2 (Ch. 4, § 3),

$$|\mathscr{C}_{\bar{G}}| = \frac{1}{|\bar{G}|} \sum_{\bar{g} \in \bar{G}} \nu(\bar{g}) .$$

$\nu(\bar{g})$ dénote le nombre de colorations φ telle que $\varphi g = \varphi$, c'est-à-dire *qui sont constantes sur chaque cycle de g.*

Il y en a donc autant que d'applications de l'ensemble des cycles — de cardinalité $\lambda_1(g) + \lambda_2(g) + \cdots$ — dans l'ensemble des m couleurs. D'où

$$|\mathscr{C}_{\bar{G}}| = \frac{1}{|G|} \sum_{g \in G} m^{\lambda_1(g)+\lambda_2(g)+\cdots} = P(G; m, ..., m, m) .$$

THÉORÈME DE POLYA. *Le nombre de schémas avec α_i objets de couleur a_i $(i = 1, 2, ..., m)$ est :*

$$\frac{1}{|G|} \sum_{\substack{\lambda_1, \lambda_2 \cdots \geqslant 0 \\ \lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n}} h_G(\lambda_1, \lambda_2, ..., \lambda_n)\, p_\alpha(\lambda_1, \lambda_2, ..., \lambda_n) .$$

$h_G(\lambda_1, \lambda_2, ..., \lambda_n)$ désigne le nombre de permutations $g \in G$ du type $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$. $p_{\alpha_1 \alpha_2 \ldots}(\lambda_1, \lambda_2, ..., \lambda_n)$ désigne le nombre de colorations qui utilisent α_i fois la couleur a_i $(i = 1, 2, ..., m)$ et qui sont constantes sur les classes d'une partition de X du type $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$;

En effet, considérons l'ensemble Φ_0 des colorations avec α_i objets de couleur $a_i (i = 1, 2, ..., m)$. L'application $\varphi \to \bar{g}(\varphi) = \varphi g$ est une injection de Φ_0 dans lui-même, donc une permutation dans Φ_0. Le nombre de schémas cherchés est comme précédemment

$$|\mathscr{C}_{\bar{G}}| = \frac{1}{|G|} \sum_{g \in G} \nu(\bar{g})$$

$\nu(\bar{g})$ dénote le nombre de colorations $\varphi \in \Phi_0$ qui sont constantes sur chaque cycle de g. Donc

$$|\mathscr{C}_{\bar{G}}| = \frac{1}{|G|} \sum_{\substack{\lambda_1, \lambda_2, \ldots, \lambda_n \geqslant 0 \\ \lambda_1 + 2\lambda_2 + \cdots = n}} \sum_{\substack{g \in G \\ g \text{ est du type} \\ 1^{\lambda_1} 2^{\lambda_2} \ldots}} p_\alpha(\lambda_1, \lambda_2, ..., \lambda_n) .$$

D'où la formule.

Exemple (Polyà). Etant données six sphères analogues,

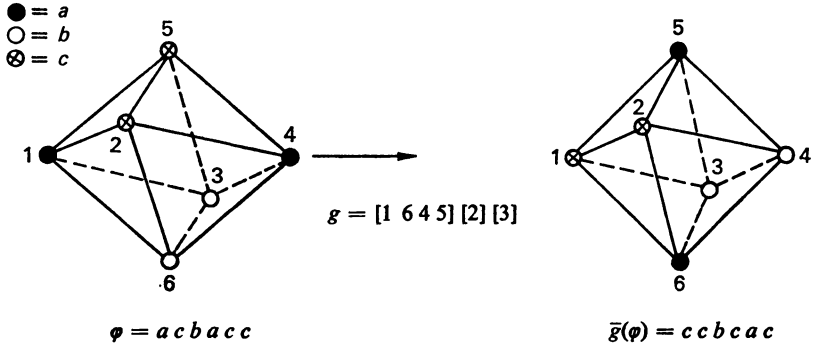
2 ayant la couleur a

1 la couleur b

3 la couleur c,

de combien de manières peut-on les répartir sur un octaèdre libre de l'espace à trois dimensions ?

Si les sommets de l'octaèdre sont numérotés 1, 2, 3, 4, 5, 6, les déplacements de l'octaèdre correspondent à des permutations de $\{ 1, 2, ..., 6 \}$; par exemple, la permutation $g = [4\ 5\ 1\ 6]\ [2]\ [3]$ correspond à une rotation de 90° autour de la diagonale 2-3 :



$\varphi = a\,c\,b\,a\,c\,c$ $\qquad$ $\bar{g}(\varphi) = c\,c\,b\,c\,a\,c$

Soit G le groupe de permutations qui correspondent à des déplacements de l'octaèdre. Le nombre de schémas est :

$$| \mathscr{C}_{\bar{G}} | = \frac{1}{| G |} \sum_{\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n} h_G(\lambda_1, \lambda_2, ..., \lambda_n)\ p_\alpha(\lambda_1, \lambda_2, ..., \lambda_n)$$

Pour l'octaèdre on obtient le tableau suivant :

Types possibles	Permutations de G du type considéré	h_G	Colorations compatibles avec le type considéré	p_α
1^6	[1] [2] [3] [4] [5] [6]	1	$(a)\,(a)\,(b)\,(c)\,(c)\,(c)$ $(a)\,(a)\,(c)\,(b)\,(c)\,(c)$ etc...	$\frac{6!}{2!\,1!\,3!} = 60$
$1^2.4$	[4 5 1 6] [2] [3] [6 1 5 4] [2] [3] [1 2 4 3] [5] [6] [3 4 2 1] [5] [6] [2 5 3 6] [1] [2] [6 3 5 2] [1] [4]	6	$\varnothing$	0
$1^2.2^2$	[4 1] [5 6] [2] [3] [1 4] [2 3] [5] [6] [2 3] [5 6] [1] [4]	3	$(b)\,(c)\,(a^2)\,(c^2)$ $(b)\,(c)\,(c^2)\,(a^2)$ $(c)\,(b)\,(a^2)\,(c^2)$ $(c)\,(b)\,(c^2)\,(a^2)$	4
2^3	[1 2] [3 4] [5 6] [1 3] [2 4] [5 6] [1 4] [2 5] [3 4] [1 4] [3 5] [2 6] [1 5] [4 6] [2 3] [1 6] [4 5] [2 3]	6	$\varnothing$	0
3^2	[1 2 5] [3 6 4] [1 2 6] [3 5 4] [1 3 5] [2 6 4] [1 3 6] [2 5 4] [1 5 2] [3 4 6] [1 6 2] [3 4 5] [1 5 3] [2 4 6] [1 6 3] [2 5 4]	8	$\varnothing$	0

D'où la réponse cherchée :

$$|\mathscr{C}_{\bar{G}}| = \frac{1}{24}(60 + 3 \times 4) = 3\,.$$

§ 2. *Dénombrement des schémas par rapport à un groupe quelconque*

Soit $X = \{ 1, 2, ..., n \}$ un ensemble de n éléments (les *objets*), $A = \{ a, b, c, ... \}$ un ensemble de m éléments (les *couleurs*), et φ une application de X dans A (ou *coloration*) ; remarquons que si g est une permutation sur X, et h une permutation sur A, l'application $h\varphi g$ est encore une coloration, soit par exemple :

$$h\varphi g = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & a & a & b & c \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & d & d & b \end{pmatrix}.$$

Considérons un groupe de permutations G sur $X \cup A$, *qui conservent X et A*, c'est-à-dire :

$$\left.\begin{matrix} (g, h) \in G \\ i \in X \end{matrix}\right\} \Rightarrow (g, h)\, i = g(i) \in X ,$$

$$\left.\begin{matrix} (g, h) \in G \\ a \in A \end{matrix}\right\} \Rightarrow (g, h)\, a = h(a) \in A .$$

Dans ce cas, on peut écrire :

$$\{ g \mid (g, h) \in G \} = G_0 , \quad \text{groupe de permutations sur } X ,$$
$$\{ h \mid (g, h) \in G \} = H_0 , \quad \text{groupe de permutations sur } A ,$$
$$G \subseteq G_0 \times H_0 .$$

Considérons enfin une famille Φ_1 de colorations qui soit *fermée* et *complète* par rapport à G, c'est-à-dire :

$$(g, h) \in G, \quad \varphi \in \Phi_1 \quad \Rightarrow \quad h\varphi g \in \Phi_1$$

$$\left.\begin{matrix} (g, h), (g', h') \in G \\ h\varphi g = h'\, \varphi g' \quad \text{pour tout} \quad \varphi \in \Phi_1 \end{matrix}\right\} \Rightarrow (g, h) = (g', h') .$$

On dira que deux colorations φ_1 et φ_2 de Φ_1 appartiennent au même *schéma par rapport au groupe G* s'il existe un $(g, h) \in G$ tel que $h\varphi_1 g = \varphi_2$; on écrira alors

$$\varphi_1 \sim \varphi_2 \quad (G)$$

Cette relation est bien une équivalence, car

$$e\varphi e = \varphi ,$$

$$h\varphi g = \varphi' \quad \Rightarrow \varphi' = h^{-1}\, \varphi g^{-1}$$

$$\left.\begin{matrix} h\varphi g = \varphi' \\ h'\varphi' g'' = \varphi'' \end{matrix}\right\} \Rightarrow \varphi'' = (h'\, h)\, \varphi(gg') .$$

On se propose ici de dénombrer les classes de cette équivalence — ou « schémas » par rapport à G —. On a le résultat suivant :

THÉORÈME GÉNÉRAL. *Le nombre de schémas pour une famille de colorations fermée et complète par rapport à un groupe $G \subseteq S_X \times S_A$ est égal à*

$$\frac{1}{|G|} \sum_{(g,h) \in G} \nu(g, h) ,$$

où $\nu(g, h)$ désigne le nombre de colorations $\varphi \in \Phi_1$ telles que les couleurs rencontrées en parcourant un cycle de g parcourant une ou plusieurs fois un même cycle de h^{-1}.

En effet, si $(g, h) \in G$ considérons l'application $t(g, h)$ définie par

$$\varphi \to t(g, h)\, \varphi = h \varphi g .$$

Si $(g, h) \in G$, on a

$$\left.\begin{array}{l} \varphi, \varphi' \in \Phi_1 \\ \varphi(k) \neq \varphi'(k) \end{array}\right\} \Rightarrow h\varphi g(g^{-1} k) \neq h\varphi'\, g(g^{-1} k) \Rightarrow t(g, h)\, \varphi \neq t(g, h)\, \varphi' .$$

L'application $t(g, h)$ étant une injection de Φ_1 dans lui-même, c'est une permutation, et le nombre de schémas est le nombre d'orbites de cette permutation, soit d'après le théorème 2 (Chap. 4, § 3) :

$$\frac{1}{|t(G)|} \sum_{(g,h) \in G} \lambda_1\big(t(g, h)\big) .$$

$\lambda_1(t(g, h))$ désigne le nombre de colorations $\varphi \in \Phi_1$ telles que $h\varphi g = \varphi$; pour un cycle $i_1, i_2, i_3, \ldots$ de g, les couleurs rencontrées seront alors :

$$\varphi(i_1) ; \quad \varphi(i_2) = h^{-1}\, \varphi(i_1) ; \quad \varphi(i_3) = h^{-1}\, \varphi(i_2) = h^{-2}\, \varphi(i_1) ; \text{ etc.}$$

Par ailleurs, l'application $(g, h) \to t(g, h)$ de G dans $t(G)$ est injective (car Φ_1 est complète par rapport à G), donc le nombre de schémas est égal à :

$$\frac{1}{|G|} \sum_{(g,h) \in G} \nu(g, h) .$$

Exemple 1. Dans le théorème de Polya on prend :

$G = G_0 \times \{ e \}$,
Φ_1 = ensemble de toutes les applications φ pour lesquelles les nombres $d_a = |\{ i / \varphi(i) = a \}|$ forment une suite de nombres donnée.

Pour calculer le nombre de rangements $R(1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n} ; 1^{\mu_1} 1^{\mu_2} \ldots m^{\mu_m})$, on prendra

$G = S_{X_1} \times S_{X_2} \times \cdots \times S_{A_1} \times S_{A_2} \times \cdots$,
Φ_1 = ensemble des applications surjectives φ de X dans A.

Exemple 2. Considérons le *problème des ménages* (Chap. 3, § 3), où $X = \{ 0, 1, 2, ..., n - 1 \}$ est un ensemble de maris, $A = \{ \underline{0}, \underline{1}, \underline{2}, ..., \underline{n - 1} \}$, leurs épouses respectives ; une bijection φ de X dans A détermine une disposition des hommes et des femmes autour d'une table ronde 0, $\varphi(0)$, 1, $\varphi(1)$, 2, etc.

Considérons les permutations circulaires de X :

$$g_p = \begin{pmatrix} 0 & 1 & 2 & \dots & n-1 \\ 0+p & 1+p & 2+p & & n-1+p \end{pmatrix}.$$

Si le numéro d'ordre de chaque personne i est diminué de p, la femme assise à la droite de l'homme $j = i - p$ sera $\varphi(i) - p$, donc φ devient φ', où

$$\varphi'(j) = \varphi(j + p) - p = g_p^{-1} \varphi g_p(j).$$

On se propose ici de dénombrer les dispositions *distinctes* des maris et des femmes autour d'une table ronde, sans place privilégiée pour l'homme 1 ; c'est donc le nombre de schémas par rapport au groupe :

$$G = \{ (g_p, g_p{}^{-1}) / p = 0, 1, 2, ..., n - 1 \}.$$

Φ_1 est l'ensemble des bijections φ qui vérifient $\varphi(i) \neq i, i + 1$. La famille Φ_1 est bien fermée et complète par rapport à G, donc le nombre de schémas est

$$\frac{1}{|G|} \sum_{g \in G} \nu(g_p, g_p^{-1}) = \frac{1}{n} \sum_{p=0}^{n-1} |\Phi_{1,p}|,$$

où $\Phi_{1,p}$ désigne la famille des colorations $\varphi \in \Phi_1$ telles que pour tout i, les couleurs rencontrées sur le cycle

$$i, i + p, i + 2p, ...$$

sont successivement

$$\varphi(i), \varphi(i) + p, \varphi(i) + 2p, ...$$

Si $p = 0$, on a, d'après la formule (§ 3, Chap. 3),

$$|\Phi_{1,0}| = |\Phi_1| = T(n) = \sum_{k=0}^{n} \frac{2n}{2n-k} (-1)^k \binom{2n-k}{k} (n-k)!$$

Si $p = 1, 2, ..., n - 1$, désignons par $(n ; p)$ le plus grand commun diviseur de n et p, et posons

$$q = \frac{n}{(n ; p)}.$$

Comme $qp \equiv 0$, les cycles de g_p sont tous de longueur q, et ce sont :

$$\begin{aligned} C_0 &= [0, p, 2p, ..., (q-1)p], \\ C_1 &= [1, 1+p, 1+2p, ..., 1+(q-1)p], \\ &\dots \\ C_{s-1} &= [s-1, s-1+p, s-1+2p, ..., s-1+(q-1)p]. \end{aligned}$$

Le nombre s de cycles distincts doit vérifier $sq = n$, donc

$$s = \frac{n}{q} = \frac{n}{\dfrac{n}{(n\,;\,p)}} = (n\,;\,p).$$

Les nombres $\varphi(0), \varphi(1), ..., \varphi(s-1)$ définissent complètement une application φ par

$$\varphi(i + kp) = \varphi(i) + kp \qquad (i = 0, 1, ..., s-1).$$

D'autre part, si pour $\varepsilon = 0$ ou 1, on a $\varphi(i) \neq i + \varepsilon$, on aura

$$\varphi(i + kp) = \varphi(i) + kp \neq (i + kp) + \varepsilon.$$

Ainsi, un $\varphi \in \Phi_{1,p}$ sera complètement déterminé par la suite

$$\varphi(0), \varphi(1), ..., \varphi(s-1)$$

(avec $\varphi(i) \neq i, i+1$), et inversement.

Soit π une permutation de 0, 1, 2, ..., $s-1$, et soit k la cardinalité de l'ensemble :

$$\{\, i \,/\, i = 0, 1, 2, ..., s-1\,; \qquad \pi(i) = i \quad \text{ou} \quad \pi(i) = i+1 \,\}.$$

On sait (Chap. 3, § 3) que le nombre de permutations π pour lesquelles k est donné est

$$T^k(s) = \sum_{j=k}^{2s} (-1)^{j-k} \binom{j}{k} \frac{2s}{2s-j} \binom{2s-j}{j} (s-j)!$$

Pour chacune de ces permutations π, cherchons combien il y a de suites $\varphi(0), \varphi(1), ...$ vérifiant $\varphi(i) \in C_{\pi_i}$ et $\varphi(i) \neq i, i+1$; il y en a exactement

$$(q-1)^k q^{s-k}.$$

Donc :

$$|\, \Phi_{1,p} \,| = \sum_{k=0}^{s} T^k(s) (q-1)^k q^{s-k}.$$

Le nombre de schémas est finalement :

$$\frac{1}{n} T^0(n) + \frac{1}{n} \sum_{p=1}^{n-1} \sum_{k=0}^{(n\,;\,p)} T^k(n\,;\,p) \left(\frac{n}{(n\,;\,p)} - 1\right)^k \left(\frac{n}{(n\,;\,p)}\right)^{(n\,;\,p)-k}.$$

Exemple 3. Le dénombrement des nœuds.

1° Considérons une ficelle dont les deux extrémités sont confondues, que l'on pose sur un plan (Cf. fig. 1) ; on suppose que chaque croisement est l'intersection de seulement deux branches, et que lorsque l'on suit la ficelle, les passages « par-dessus » et les passages « par-dessous » alternent.

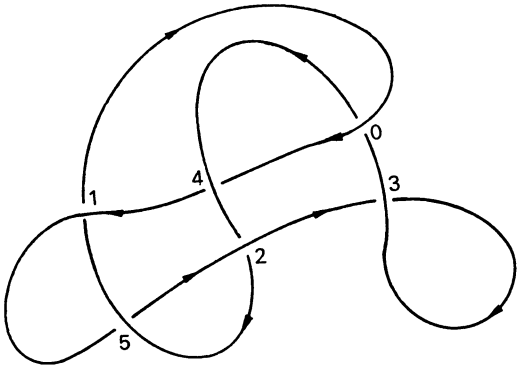


FIG. 1.

Lorsqu'un tel schéma est réalisé, on dit que l'on a un *nœud* alterné. Pour décrire un nœud alterné, choisissons arbitrairement un croisement que l'on note 0 ; puis suivons la branche supérieure dans une direction arbitraire, jusqu'au prochain passage « par-dessus » ; dénotons par 1 ce nouveau croisement, et continuons de la même façon à numéroter les autres croisements supérieurs successivement rencontrés : 2, 3, 4, ... Le nœud définit alors une bijection φ, ou l'image $\varphi(i)$ du croisement supérieur i est le croisement inférieur $\underline{j}$ qui le suit immédiatement. Par exemple, pour la figure 1, la bijection obtenue est :

$$\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ \underline{4} & \underline{5} & \underline{3} & \underline{0} & \underline{2} & \underline{1} \end{pmatrix}.$$

2° Si, en parcourant la ficelle, le croisement supérieur i est immédiatement suivi du croisement inférieur $\underline{i}$, c'est-à-dire si $\varphi(i) = \underline{i}$, on se trouve sur une « boucle », qui peut être éliminée par simple retournement. Il sera de même, si $\varphi(i) = \underline{i+1}$ (comme c'est le cas pour le nœud de la figure 1 pour $i = 2$).

En d'autres termes, nous supposerons que la permutation φ définie par le nœud *satisfait aux conditions du problème des ménages.*

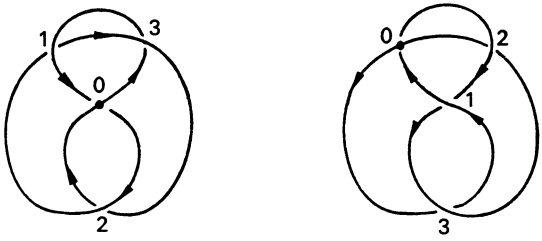
En outre, si l'on choisit pour le point 0 un autre croisement, cela revient à changer φ en $\varphi' = g_p^{-1}\,\varphi g_p$; si l'on renverse le sens du parcours de la ficelle, cela revient à changer φ en $\varphi' = h^{-1}\,\varphi h$, où

$$h = [n-1, 1]\,[n-2, 2]\,[n-3, 3]\ldots$$

Dans de tels cas, les permutations φ et φ' seront dites *équivalentes*. Un nœud alterné à n croisements ne définit donc pas une permutation de degré n, mais une classe d'équivalence, appelée la *signature* du nœud. Le nombre de signatures de degré n découle immédiatement de la formule obtenue dans l'exemple précédent. On trouve les valeurs :

$n =$	3	4	5	6	7	8	9
	1	2	5	20	87	616	4 843

3° Une application pratique de cette théorie est le problème suivant. Considérons deux nœuds alternés (I) et (II) de degré n : est-il possible de passer de l'un à l'autre en déplaçant la ficelle sans jamais créer de nouveaux croisements, et sans que les croisements ne quittent le plan ? Considérons les deux nœuds suivants :



(I) (II)

FIG. 2.

On constate sans peine qu'ils sont images dans un miroir l'un de l'autre, cependant, ils définissent tous deux la permutation :

$$\varphi = \begin{pmatrix} 0\,1\,2\,3 \\ 3\,0\,1\,2 \end{pmatrix}.$$

On peut donc passer de l'un à l'autre par déplacement des croisements sur le plan (ce qui ferait dire à Lewis Caroll qu'une telle manipulation lui fait traverser le miroir !).

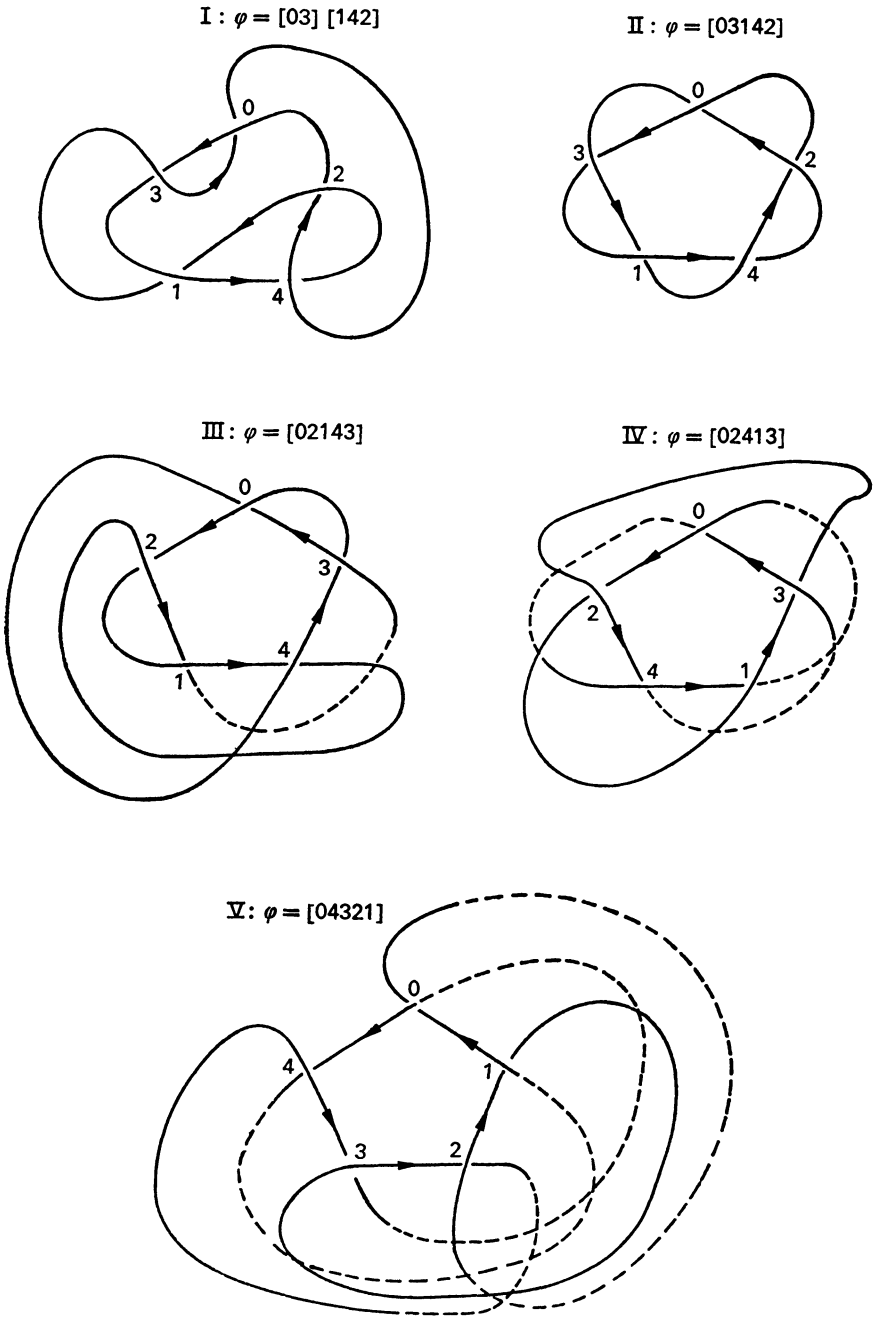


FIG. 3. — Les 5 signatures de degré 5.

4° D'une façon plus générale, un *nœud d'ordre n* est un nœud qui, posé sur le plan, présente n croisements (et ne peut pas en présenter moins).

Deux nœuds N et N' seront dits identiques si on peut les amener à coïncider par déplacements (c'est-à-dire, s'il existe un homéomorphisme de R^3 dans lui-même qui applique N sur N').

Il existe de nombreux travaux sur la classification des nœuds (cf. par exemple la bibliographie de Fox (1963), ou, plus récemment, le livre de L. P. Neurwirth, *Knot groups*, Princeton Univ. Press, 1965). Malheureusement, tout nœud n'est pas un nœud alterné. En outre, toute signature de degré n ne définit pas un nœud alterné d'ordre n, comme on peut le voir sur la figure 3.

§ 3. *Un théorème de De Bruijn*

Soit $\varphi_0 \in \Phi$ une coloration et $\overline{\varphi}_0$ son schéma par rapport à un groupe G de permutations sur X ; l'ensemble des colorations φ avec $\overline{\varphi} = \overline{\varphi}_0$ peut s'écrire :

$$\{ \varphi \,/\, \varphi \in \Phi,\ \varphi g = \varphi_0 \quad \text{pour un} \quad g \in G \} .$$

Si le schéma $\overline{\varphi}_0$ ne change pas lorsque les couleurs subissent une permutation h, cela s'écrit $h\varphi_0 \in \varphi_0\, G$.

A chaque objet de couleur a assignons un *poids* $w(a) > 0$; à un schéma $\overline{\varphi}$ où la couleur a_i figure r_i fois (pour $i = 1, 2, ..., m$), assignons le *poids*

$$W(\overline{\varphi}) = w(a_1)^{r_1}\, w(a_2)^{r_2} \ldots w(a_m)^{r_m} .$$

On se propose ici d'évaluer la somme des poids de tous les schémas qui restent invariants dans une permutation h. Si l'on fait $w(a) = 1$ pour tout a, l'on obtient le nombre de schémas invariants dans la permutation h.

Théorème de De Bruijn. *La somme des poids de tous les schémas invariants dans une permutation h des couleurs est*

$$\sum W(\overline{\varphi}) = P(G\,;\, p_1, p_2, ..., p_n) ,$$

où

$$P(G\,;\, x_1, x_2, ..., x_n) = \frac{1}{|\,G\,|} \sum_{g \in G} (x_1)^{\lambda_1} (x_2)^{\lambda_2} \ldots (x_n)^{\lambda_n}$$

est l'indicateur de cycles de G, et où

$$p_k = \sum_{\substack{a \in A \\ h^k a = a}} w(a)\, w(ha)\, w(h^2 a) \ldots w(h^{k-1} a) .$$

1) Considérons un schéma $\overline{\varphi}_0$ qui ne change pas lorsque les couleurs subissent une permutation h, c'est-à-dire avec $h\varphi_0 \in \varphi_0\, G$.

On a :

$$\overline{\varphi} = \overline{\varphi}_0 \quad \Rightarrow \quad \varphi \in \varphi_0 G \quad \Rightarrow \quad h\varphi = h\varphi_0 g = \varphi_0 g_0 g \in \varphi_0 G \quad \Rightarrow \quad \overline{h\varphi} = \overline{\varphi}_0 .$$

Inversement,

$$\overline{h\varphi} = \overline{\varphi}_0 \Rightarrow \begin{cases} h\varphi \in \varphi_0 G \\ h\varphi_0 \in \varphi_0 G \end{cases} \Rightarrow \begin{cases} \varphi = h^{-1} \varphi_0 g \\ \varphi_0 = h^{-1} \varphi_0 g_0 \end{cases} \Rightarrow \varphi = h^{-1} \varphi_0 g_0 (g_0^{-1} g) \in \varphi_0 G$$

$$\Rightarrow \overline{\varphi} = \overline{\varphi}_0 .$$

Donc les colorations du même schéma que φ_0 sont les φ avec $\overline{h\varphi} = \overline{\varphi}_0$.

2) L'application $\varphi \to h\varphi g = \overline{g}(\varphi)$ est une permutation sur Φ car

$$\varphi \neq \varphi' \quad \Rightarrow \quad h\varphi g \neq h\varphi' g ;$$

l'orbite du groupe $\overline{G} = \{ \overline{g} \,/\, g \in G \}$ qui contient φ_0 est :

$$O(\varphi_0) = \{ \varphi \,/\, h\varphi g = \varphi_0 \quad \text{pour un} \quad g \in G \} = \{ \varphi \,/\, \overline{h\varphi} = \overline{\varphi}_0 \} .$$

On a par conséquent (Théorème 1, Chap. 4, § 3) :

$$\sum W(\overline{\varphi}) = \sum_{\varphi \,/\, h\varphi \in \varphi G} \frac{W(\varphi)}{|O(\varphi)|} = \frac{1}{|\overline{G}|} \sum_{h\varphi \in \varphi G} W(\varphi) \, |\overline{G}_\varphi|$$

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{\varphi \,/\, h\varphi \in \varphi G \\ h\varphi g = \varphi}} W(\varphi) = \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{\varphi \\ h\varphi g = \varphi}} W(\varphi)$$

(car $h\varphi g = \varphi$ entraîne $h\varphi = \varphi g^{-1} \in \varphi G$).

3) Si g est une permutation sur X du type $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$, dont les cycles forment une partition $(Y_1, Y_2, \ldots, Y_s)$, choisissons une suite $y_1 y_2 \ldots y_s$ avec :

$$y_i \in Y_i \qquad (i = 1, 2, \ldots, s) .$$

Si $h\varphi g = \varphi$, et si $k(i)$ est la longueur du cycle de g contenant y_i, les couleurs de Y_i sont

$$\varphi(y_i) = a , \quad \varphi g^{-1}(y_i) = ha , \quad \ldots \quad \varphi g^{-k(i)}(y_i) = h^k a = a .$$

Donc

$$W(\varphi) = \prod_{i=1}^{s} p_{k(i)}(\varphi(y_i)) ,$$

en posant

$$p_k(a) = w(a)\, w(ha)\, w(h^2 a) \ldots w(h^{k-1} a) \qquad \text{si } a = h^k a$$

$$= 0 \qquad \text{si } a \neq h^k a .$$

4) Posons

$$A_k = \{ a \mid a \in A ; h^k a = a \} = \{ a_k^1, a_k^2, ..., a_k^{p_k} \} .$$

Si l'on remarque que φ est complètement déterminé par le s-uple $(j_1 j_2 ... j_s)$ par

$$\varphi(y_i) = a_{k(i)}^{j_i} \qquad (i = 1, 2, ..., s) ,$$

l'on peut écrire

$$\begin{aligned} \sum_{h\varphi g = \varphi} W(\varphi) &= \sum_{(j_1, j_2, ..., j_s)} p_{k(1)}(a_{k(1)}^{j_1})\, p_{k(2)}(a_{k(2)}^{j_2}) \cdots p_{k(s)}(a_{k(s)}^{j_s}) \\ &= \prod_{i=1}^{s} [p_{k(i)}(a_{k(i)}^1) + p_{k(i)}(a_{k(i)}^2) + \cdots] \\ &= \prod_{i=1}^{s} \sum_{a \in A_{k(i)}} w(a)\, w(ha) \ldots w(h^{k(i)-1} a) \\ &= \prod_{i=1}^{s} p_{k(i)} = (p_1)^{\lambda_1} (p_2)^{\lambda_2} \ldots (p_n)^{\lambda_n} . \end{aligned}$$

D'où la formule annoncée.

Exemple. Dans le cas de la coloration du cube (Exemple 1, § 1), on a déterminé plus haut le groupe G des rotations du cube, ce qui donne pour indicateur de cycles :

$$P(G ; x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}(x_1^6 + 3\, x_1^2\, x_2^2 + 6\, x_1^2\, x_4 + 6\, x_2^3 + 8\, x_3^2) .$$

Le nombre de schémas en deux couleurs a, b répartis d'une façon symétrique est obtenu en faisant $h = [ab]$, $w(a) = w(b) = 1$; c'est donc :

$$P(G ; 0, 2, 0, 2, 0, 2) = \frac{1}{24}(6.2^3) = 2 .$$

Cherchons le nombre de façons de colorer les 6 faces avec 6 couleurs distinctes $a_1, a_1', a_2, a_2', a_3, a_3'$ de sorte que la permutation $h = [a_1\, a_1']\ [a_2\, a_2']\ [a_3\, a_3']$ laisse invariant le « schéma » (c'est-à-dire : le cube libre de l'espace à trois dimensions). Posons pour simplifier $w(a_i) = w_i$, $w(a_i') = w_i'$, et calculons les p_k :

$$\begin{aligned} p_1 &= 0 \\ p_2 &= 2\, w_1\, w_1' + 2\, w_2\, w_2' + 2\, w_3\, w_3' \\ p_3 &= 0 \\ p_4 &= 2(w_1)^2\, (w_1')^2 + 2(w_2)^2\, (w_2')^2 + 2(w_3)^2\, (w_3')^2 \\ p_5 &= 0 \\ p_6 &= 2(w_1)^3\, (w_1')^3 + 2(w_2)^3\, (w_2')^3 + 2(w_3)^3\, (w_3')^3 . \end{aligned}$$

Le nombre cherché est le coefficient de $w_1\, w_1'\, w_2\, w_2'\, w_3\, w_3'$ dans le polynôme :

$$P(G\,;\, p_1, p_2, p_3, p_4, p_5, p_6) = \frac{1}{24} 6\, p_2^3$$

$$= \frac{2^3}{4} (w_1\, w_1' + w_2\, w_2' + w_3\, w_3')^3$$

$$= 2 \sum_{\alpha+\beta+\gamma=3} \frac{3!}{\alpha!\,\beta!\,\gamma!} (w_1\, w_1')^\alpha\, (w_2\, w_2')^\beta\, (w_3\, w_3')^\gamma .$$

Il y a donc 12 possibilités.

COROLLAIRE 1 (Polyà). *Si l'on pose* $w_i = w(a_i)$, *la somme des poids de tous les schémas relatifs à un groupe G de permutations des objets est :*

$$\sum W(\overline{\varphi}) = P\left(G\,;\, \sum_{i=1}^{m} w_i,\, \sum_{i=1}^{m} w_i^2,\, \sum_{i=1}^{m} w_i^3 \ldots\right).$$

Le nombre de schémas $\overline{\varphi}$ *qui utilisent* α_i *fois la couleur* a_i (pour $i = 1, 2, \ldots, m$) *est donc le coefficient de* $w_1^{\alpha_1}\, w_2^{\alpha_2} \ldots w_m^{\alpha_m}$ *dans le polynôme ci-dessus.*

(D'après le théorème précédent, en prenant pour h la permutation unité.)

COROLLAIRE 2 (de Bruijn). *Soient* G_0, H_0 *deux groupes de permutations sur X et sur A, et assignons à chaque schéma* φ *par rapport au groupe*

$$G = G_0 \times H_0$$

un poids comme précédemment. La somme des poids des différents schémas est

$$\sum W(\overline{\varphi}) = \frac{1}{|H_0|} \sum_{h \in H_0} P(G_0\,;\, p_1(h), p_2(h), \ldots)$$

$$p_k(h) = \sum_{h_k a = a} w(a)\, w(ha) \ldots w(h^{k-1} a) .$$

En effet, on peut voir comme précédemment que

$$\sum W(\overline{\varphi}) = \frac{1}{|H_0|} \sum_{h \in H_0} \sum_{\substack{\overline{\overline{\varphi}} \\ h\varphi \in \varphi G}} W(\overline{\overline{\varphi}})$$

où dans la dernière somme $\overline{\overline{\varphi}}$ désigne un schéma par rapport à G_0 invariant dans la permutation h des couleurs.

APPLICATION. *Dénombrement des graphes à sommets non étiquetés.*

Si G est un groupe de permutations agissant sur un ensemble X, on peut considérer l'ensemble $\mathscr{P}'_2(X)$ des paires $\{ x, y \}$, avec $x, y \in X$, $x \neq y$.

Une permutation $g \in G$ induit sur $\mathscr{P}'_2(x)$ une application $\bar{g}$, où

$$\bar{g}(x, y) = \{ g(x), g(y) \} .$$

$\bar{g}$ est une permutation, dont l'ensemble forme un groupe noté $G^{(2)}$. Deux graphes (X, U) et (X, V) seront dits *isomorphes* s'il existe une permutation g des sommets telle que

$$(x, y) \in U \Leftrightarrow \bar{g}(x, y) \in V .$$

Un *graphe à sommets non étiquetés* (unlabelled graphs) est une classe d'isomorphie. On se propose de compter les graphes non isomorphes à n sommets.

$\mathscr{P}'_2(X)$ est l'ensemble des $\dfrac{n(n-1)}{2}$ arêtes du graphe complet de sommets $x_1, x_2, ..., x_n$ (sans boucles ni arêtes multiples). A toute application φ de $\mathscr{P}'_2(X)$ dans un ensemble $A = \{ a, b \}$ de deux couleurs correspond un graphe (X, U) par

$$U = \{ u \mid u \in \mathscr{P}'_2(X), \varphi(u) = a \} .$$

Cette correspondance est bijective.

Donc le nombre de graphes (à sommets non étiquetés) de n sommets est

$$P(S_n^{(2)} ; 2, 2, 2, ...) . \qquad \text{(Théorème 1, § 1)}$$

Le nombre de graphes isomorphes à leurs complémentaires est

$$P(S_n^{(2)} ; 0, 2, 0, 2, ...) \qquad \text{(Théorème, § 3)}$$

Le nombre de découpages en deux classes des arêtes d'un graphe complet (à sommets non étiquetés) est

$$\tfrac{1}{2} P(S_n^{(2)} ; 2, 2, 2, ...) + \tfrac{1}{2} P(S_n^{(2)} ; 0, 2, 0, 2, ...) \quad \text{(Corollaire 2, § 3).}$$

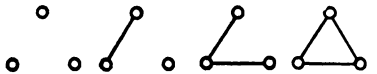
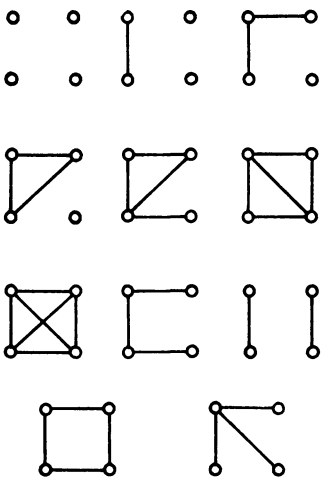
Le nombre de graphes (à sommets non étiquetés) de n sommets et m arêtes est le coefficient de w^m dans

$$P(S_n^{(2)} ; 1 + w, 1 + w^2, 1 + w^3, ...) \qquad \text{(Corollaire 1, § 3).}$$

Le nombre de graphes auto-complémentaires à m arêtes est le coefficient de w^m dans

$$P(S_n^{(2)} ; 0, 2w, 0, 2w^2, 0, 2w^3, ...) \qquad \text{(Théorème, § 3).}$$

Si l'on dénombrait les graphes orientés, il suffirait de remplacer $S_n^{(2)}$ par le produit cartésien $S_n \otimes S_n$.

$n =$	Graphes non étiquetés	$P(S_n^{(2)}; x_1, x_2, \ldots)$	$P(S_n^{(2)}; 2, 2, \ldots)$	$P(S_n^{(2)}; 0, 2, 0, 2, \ldots)$	$P(S_n^{(2)}; 1+w, 1+w^2, \ldots)$
2		x_1	2	0	$1 + w$
3		$\frac{1}{6}(x_1^3 + 3\,x_1 x_2 + 2\,x_3)$	4	0	$1 + w + w^2 + w^3$
4		$\frac{1}{24}(x_1^6 + 9\,x_1^2 x_2^2 + 8\,x_3^2 + 6\,x_2 x_4)$	11	1	$1 + w + 2\,w^2 + 3\,w^{3'} + 2\,w^4 + w^5 + w^6$

§ 4. *Calcul de l'indicateur de cycles*

Nous nous proposons maintenant d'indiquer sans démonstration détaillée les principales formules (d'après [9]) permettant de calculer le polynôme $P(G\,;\,x_1, x_2, \ldots, x_n) = P(G)$.

1° *Le groupe symétrique* S_n a pour ordre $n\,!$

D'après la formule de Cauchy (Chap. 4, § 2), on a

$$P(S_n) = \sum_{\lambda_1 + 2\lambda_2 + \cdots = n} \frac{1}{\lambda_1!\, 2^{\lambda_2}\, \lambda_2! \ldots n^{\lambda_n}\, \lambda_n!}\, x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n}.$$

2° Le *groupe alterné* A_n consiste en toutes les permutations paires de n objets, et a pour ordre $\frac{n\,!}{2}$; on a immédiatement :

$$P(A_n) = \sum_{\lambda_1 + 2\lambda_2 + \cdots = n} \frac{1 + (-1)^{\lambda_2 + \lambda_4 + \lambda_6 \ldots}}{\lambda_1!\, 2^{\lambda_2}\, \lambda_2! \ldots n^{\lambda_n}\, \lambda_n!}\, x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n}.$$

3° Le *groupe identité* $E_n = \{ e \}$, qui contient seulement la permutation identique e, donne :

$$P(E_n) = x_1^n .$$

4° Le *groupe cyclique* C_n a pour ordre n, et est engendré par la permutation circulaire $[1,\ 2, \ldots, n]$.

$$P(C_n) = \frac{1}{n} \sum_{k \,/\, n} \varphi(k)\, (x_k)^{\frac{n}{k}},$$

où $\varphi(k)$ est la fonction d'Euler donnée au chapitre 3, § 3.

5° Le *groupe dihédral* D_n a pour ordre $2\,n$, et est engendré par les deux permutations $[1, 2, \ldots, n]$ et $[1, n]\,[2, n-1]$...

Si n pair $= 2\,p$ on a :

$$P(D_{2p}) = \frac{1}{4\,p} \sum_{k \,/\, 2p} \varphi(k)\, (x_k)^{\frac{2p\,/\,k}{k}} + \frac{1}{4}\,(x_2^p + x_1^2\, x_2^{p-1}) .$$

Si n impair $= 2\,p + 1$:

$$P(D_{2p+1}) = \frac{1}{2(2\,p+1)} \sum_{k \,/\, 2p+1} \varphi(k)\, x_k^{2p+1\,/\,k} + \frac{1}{2}\, x_1\, x_2^p .$$

6° Le *produit simple* $G \times H$; si G est un groupe de permutations d'ordre r

sur X, H un groupe de permutations d'ordre s sur Y ($|X| = p$, $|Y| = q$), le produit simple agit sur $X \cup Y$ par

$$(g, h)\, z = \begin{cases} gz & \text{si} \quad z \in X, \\ hz & \text{si} \quad z \in Y. \end{cases}$$

Son ordre est rs, et l'on a

$$P(G \times H) = P(G) \times P(H).$$

7° Le *produit cartésien* $G \otimes H$. Il agit sur $X \times Y$ par :

$$(g, h)\,(x, y) = (gx, hy).$$

Son ordre est rs.

Supposons que x est sur un circuit de longueur k du graphe de g, et g sur un circuit de longueur l du graphe de h ; alors (x, y) est sur un circuit de longueur $m(k, l)$, le p. p. c. m. des nombres k et l ; le nombre de tels cycles est $(k\,;\, l)$, le p. g. c. d. des nombres k et l. Donc

$$P(G \otimes H) = \frac{1}{|G|.|H|} \sum_{g,h} \prod_{k,l} x_{m(k,l)}^{(k\,;\,l)\lambda_k(g)\lambda_l(h)}$$

8° Le *produit de composition* $G[H]$ agit sur $X \times Y$, et contient les permutations $t(g\,;\, h_1, h_2, ..., h_n)$ définies par :

$$t(g\,;\, h_1, h_2, ..., h_n)\,(x_i, y) = (gx_i, h_i\, y).$$

Son ordre est $r.s^p$; Polyà a montré :

$$P\big(G[H]\big) = P\big(G\,;\, p_1(H), p_2(H), ...\big)$$

où $p_k(H) = P(H\,;\, x_k, x_{2k}, x_{3k}, ...)$.

9° La *puissance* H^G agit sur l'ensemble Y^X de toutes les applications de X dans Y par :

$$t(g, h) f(x) = hfg(x).$$

Son ordre est rs et son polynôme est :

$$P(H^G) = \frac{1}{|G|.|H|} \sum_{\substack{g \in G \\ h \in H}} \prod_{k=1}^{q^p} x_k^{\lambda_k(g,h)}.$$

Ici, on a

$$\lambda_1(g, h) = \prod_{k=1} \sum_{r/k} [r\lambda_r(h)]^{\lambda_k(g)}.$$

Pour $k > 1$, on trouve, en utilisant la formule d'inversion de Möbius :

$$\lambda_k(g, h) = \frac{1}{k} \sum_{r/k} \mu(r, k)\, \lambda_1(g^r, h^r).$$

BIBLIOGRAPHIE

Chapitre 1

[1] E. T. BELL, Exponential polynomials, *Ann. of Math.*, II, **35**, 1934, pp. 258-277.
[2] C. BERGE, *Théorie des graphes et ses applications*. Paris, Dunod 1958.
[3] C. BERGE, Sur un nouveau calcul symbolique et ses applications, *Journ. de Math. Pures et Appl.*, **29**, 1950, pp. 245-274.
[4] P. ERDÖS, G. SZEKERES, A Combinatorial problem in Geometry, *Compositio Math.*, **2**, 1935, pp. 463-470.
[5] C. FRASNAY, Quelques problèmes combinatoires concernant les ordres totaux, Thèse, Paris, 1967.
[6] J. RIORDAN, *Introduction to Combinatorial Analysis*, J. Wiley, N. Y. 1958.
[7] G. C. ROTA, The number of partitions of a set, *Am. Math. Monthly*, **71**, 1964, pp. 498-504.
[8] H. J. RYSER, *Combinatorial Mathematics*, Buffalo, Mathematical Ass. of America, 1963. Traduction française par P. Camion, Dunod, 1968.
[9] J. TOUCHARD, Nombres exponentiels et nombre de Bernoulli, *Canad. J. Math.*, **8**, 1956, pp. 305-320.
[10] A. KAUFMANN, *Initiation à la combinatorique*, Paris, Dunod, 1968.

Chapitre 2

[1] E. T. BELL, *Algebraic Arithmetic*, New York, Americ. Math. Soc., 1927.
[2] P. BERTIER, Partages, parties, partitions. Décomptes et représentations, *Metra*, **6**, 1967, pp. 103-129.
[3] J. S. FRAME, G. de B. ROBINSON, R. M. THRALL, The Hook Graphs of the Symmetric Groups, *Canad. Journ. of Math.*, **6**, 1954, pp. 316-323.
[4] G. Th. GUILBAUD, Un problème leibnizien : les partages en nombres entiers, *Mathématiques et Sciences Humaines*, **17**, 1966, pp. 13-16.
[5] G. KREWERAS, Sur une classe de problèmes de dénombrement liés au treillis des partitions des entiers, *Cahiers du BURO*, **6**, ISUP, 1965, pp. 9-103.
[6] P. A. MAC-MAHON, *Combinatory Analysis*, Cambridge 1915-1916, réimpr. Chelsea, New York, 1960.
[7] F. D. MURNAGHAM, *The Theory of Group Representation*, Baltimore, 1928.
[8] G. DE B. ROBINSON, On the Representation of the Symmatric Group. *Am. J. Math.* **60**, 1938, pp. 745-760.
[9] D. E. RUTHERFORD, *Substitional Analysis*, Edinburgh, 1948.
[10] C. SCHENSTED, Longest Increasing and Decreasing Subsequences, *Canad. Journal of Math.*, **13**, 1961, pp. 179-191.
[11] M. P. SCHÜTZENBERGER. Quelques remarques sur une construction de Schensted, *Math. Scandinavica*, **12**, 1963, pp. 117-128.
[12] E. M. WRIGHT, Partition of Multipartite Number into k parts, *J. Reine Angew. Math.*, **216**, 1964, pp. 101-112.
[13] A. YOUNG, On Quantitative Substitutional Analysis, *Proc. London Math. Soc.*, **34**, 1902, pp. 361-397.
[14] A. YOUNG, On Quantitative Substitutional Analysis, *Proc. London Math. Soc.* (2), **28**, 1927, pp 255-292.

Chapitre 3

[1] L. CARLITZ, Rings of Arithmetic Functions, *Pacific J. Math*, **14**, 1964, pp. 1165-1171.
[2] A. CAYLEY, A theorem on trees, *Quart. J. Math.*, **23**, 1889, pp. 376-378.
[3] L. E. CLARKE, On Cayley's Formula for Counting Trees, *J. London Math. Soc.*, **33**, 1958, pp. 471-475.
[4] S. GLICKSMAN, On the Representation and Enumeration of Trees, *Proc. Camb. Phil. Soc.*, **59**, 1963, pp. 509-517.
[5] I. KAPLANSKI et J. RIORDAN, The problème des ménages, *Scripta Math.*, **12**, 1946, pp. 113-124.
[6] H.MEIER-WUNDERLI, Note on a Basis of P. HALL for Higher Commutation in tree Groups *comment. Helvatici Math.*, **26**, 1952, pp. 1-5.
[7] V. V. MENON, On the existence of trees with given degrees, Sankhya, **26**, 1964, pp. 63-68.
[8] A. F. MÖBIUS, Über eine besondere Art von Umkehrung der Reihen, *J. Reine Angew. Math.*, **9**, 1832, 105-123.
[9] J. W. MOON, Enumerating Labelled Tress, in *Graph Theory and Theoretical Physics*, par F. Harary, Academic Press, London and New York, 1967, pp. 261-271.
[10] J. W. MOON, On the second moment of the complexity of a graph, Mathematika, **11**, 1964, 95-98.
[11] C. MOREAU. Cité par E. LUCAS, Théorie des nombres, Gauthiers-Villars, Paris 1891, pp. 396-397.
[12] P. V. O'NEILL, The number of trees in a certain network, *Notices Amer. Math. Soc.* **10**, 1963, p. 569.
[13] A. RÉNYI, Some Remarks on the Theory of Trees, *Magy. Tudom. Akad. Mat. Kut. Intéz. Kölz.*, **4**, 1959 a, pp. 73-85.
[14] G. C. ROTA, (Communication privée).
[15] G. C. ROTA, On the Foundations of Combinatorial Theory I. Theory of Möbius Functions, *Zeitschrift für Wahrscheinlichkeitstheorie*, Band 2, Heft 4, 1964, pp. 340-368.
[16] M. P. SCHÜTZENBERGER, Contribution aux applications statistiques de la théorie de l'information, *Publ. Inst. Stat. Univ. Paris*, **3**, 1954, pp. 5-117.
[17] H. I. SCOINS, The number of Trees with Nodes of Alternate Parity, *Proc. Camb. Phil. Soc.*, **58**, 1962, pp. 12-16.
[18] D. A. SMITH, Incidence functions as generalized arithmetic functions, *Duke Math. J.*, **34**, 1967, pp. 617-633.
[19] H. N. V. TEMPERLEY, On the Mutual Cancellation of Cluster Integrals in Mayer's Fugacity Series, *Proc. Phys. Soc.*, **83**, 1964, pp. 3-16.
[20] J. TOUCHARD, Sur un problème de permutations, *C. R. Acad. Sci. Paris*, **198**, 1943, pp. 631-633.
[21] L. WEINBERG, Number of Trees in a Graph, *Proc. IRE*, **46**, 1958, pp. 1954-1955.
[22] C. BERGE, *Théorie des Graphes et ses Applications*, Paris, 1958.

Chapitre 4

[1] G. Th. GUILBAUD, et P. ROSENSTHIEL. Analyse algébrique d'un scrutin. *Math. et Sc. Humaines*, **4**, 1960, pp. 9-33.
[2] P. ROSENSTIEHL. Communication au colloque NATO sur la Théorie des Jeux, Toulon, 1966.
[3] H. WIELANDT. *Finite Permutation Groups*, Academic Press, New York 1964.

Chapitre 5

[1] N. G. de BRUIJN, Color Patterns that are Invariant under a given Permutation of the Colors, *Journal of Comb. Theory*, **2**, n° 4, 1967, pp. 418-421.

[2] N. G. de BRUIJN, Generalization of Polyà's Fundamental Theorem in Enumerative Combinatorial Analysis, *Nederl. Akad. Wetensch. Proc.*, Ser A, **62** ; *Indagationes Mathematicae*, **21**, 1959, pp. 59-69.

[3] N. G. de BRUIJN, Polyà's Theory of Counting, *Applied Combinatorial Mathematics*, chap. 5 (E. F. Beckenbach, éd.), Wiley, New York, 1964.

[4] G. DEMOUCRON, Y. MALGRANGE, R. PERTUISET, Reconnaissance et construction de représentations planaires topologiques, *Revue Française de R. O.*, 1964, **30**, pp. 33-47.

[5] J. DÉNES, The Representation of a Permutation as the Product of a Minimal Number of Transpositions, and its Connection with the Theory of Graphs, *Math. Inst. of the Hungarian Ac. of Science*, 1959, **4**, fasc. 1.

[6] M. EDEN, M. P. SCHÜTZENBERGER, Remark on a Theorem of Dénes, *Math. Institute of the Hungarian Academy of Sciences*, 1962, **7**, sér. A, fasc. 3.

[7] E. N. GILBERT, Knots and Classes of Ménage Permutations, *Scripta Mathematica*, 1956, **22**, pp. 228-233.

[8] F. HARARY, The number of Linear, Directed, Rooted and Connected Graphs, *Trans. Amer. Math. Soc.*, 1955, **78**, pp. 445-463.

[9] F. HARARY, Graphical Enumeration Problems, in BECKENBACH, *Applied Combinatorial, Mathematics*, Wiley, New York, 1966.

[10] F. HARARY, Unsolved Problems in the Enumeration of Graphs, *Publ. Math. Inst. Hungar. Acad. Sci.*, 1960, **5**, pp. 63-95.

[11] I. KAPLANSKY, J. RIORDAN, *Le Problème des ménages*, Scripta Mathematica, 1946, **12**, pp. 113-124.

[12] A. LEMPEL, S. EVEN, I. CEDERBAUM, An Algorithm for Planarity Testing of Graphs, Séminaire de Rome, *Théorie des Graphes*, Dunod 1967, p. 215-232.

[13] G. POLYÀ, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen, *Acta Math.*, 1937, **68**, pp. 145-254.

[14] J. RIGUET, Notice sur quelques principes fondamentaux d'énumération, in Claude BERGE, *Théorie des Graphes*, Dunod, 1958.

[15] P. G. TAIT, *Scientific Papers*, Cambridge 1898, **3**, vol. 1, p. 287.

Imprimé en France. — Imprimerie JOUVE, 12, rue de Tournon, PARIS (6e)
Dépôt légal : N° 5845, 3e trimestre 1968

PRINCIPES DE COMBINATOIRE