SUR LES CYCLES DES SUBSTITUTIONS.

Par

JACQUES TOUCHARD

à Paris.

Introduction.

Certaines questions d'analyse combinatoire, comme le problème des rencontres, traité par Euler, ou comme son extension, traitée par Sylvester, conduisent à rechercher, d'une manière plus générale, quel est le nombre u_n des substitutions de n lettres ou de n indices dont les cycles possèdent une certaine propriété. Telle est l'origine du présent travail.

La nature des propriétés attribuables aux cycles ayant été préalablement précisée, nous serons en mesure, au § I, d'établir des formules récurrentes propres au calcul numérique des nombres u_n. A l'aide de ces formules, on peut soit remonter aux fonctions génératrices

$$\sum_{n=0}^{n=\infty} u_n \frac{z^n}{n!},$$

soit se borner à obtenir, de proche en proche, des expressions algébriques que nous désignerons, avec M. G. Pólya, sons le nom d'indicateurs de cycles et qui mettent, en effet, en évidence la constitution de certaines familles de substitutions au moyen de leurs cycles jouissant des propriétés envisagées.

Il se trouve que certains polynômes étudiés autrefois par Appell[1] et, en particulier, les polynômes d'Hermite ou, du moins, des polynômes qui s'en déduisent par un changement de variable immédiat, peuvent être considérés comme des indicateurs de cycles. C'est ce que nous établissons, entre autres choses, dans notre § II.

---

[1] P. Appell. — Ann. Ec. Norm. sup. T. IX, 1880, p. 119.

Le § III étend les principaux résultats du § I à des substitutions prises dans le groupe alterné de degré n ou dans certaines familles, analogues, à quelques égards, aux ensembles des substitutions paires ou impaires.

Dans les § IV et V, nous définissons ce que nous entendons par une substitution à cycles monotones et par cycles secondaires d'une substitution. Nous déterminons le nombre des substitutions qui admettent une décomposition donnée en cycles secondaires et nous résolvons ensuite, relativement à ceux-ci, certains problèmes traités au § I, pour les cycles primaires. En particulier, nous établissons des formules indicatrices de cycles secondaires.

Le § VI conduit, par l'examen attentif des solutions de certaines équations différentielles linéaires, du second on du troisième ordre, ou même d'ordre supérieur, à répartir les cycles primaires des substitutions entre diverses catégories. Ces catégories, qui se présentent naturellement et qui dépendent des rapports mutuels de deux ou de plusieurs cycles, sont envisagées ici pour la première fois et il ne nous est pas encore possible, après cette étude sommaire, de savoir si leur intervention pourra ou non être de quelque utilité dans la théorie des groupes d'ordre fini.

Enfin le § VII est consacré à quelques applications; notamment à l'évaluation asymptotique de l'ordre moyen d'un cycle primaire ou secondaire, dans le groupe symétrique, ou encore à celle de l'ordre moyen d'un cycle appartenant à une des catégories que nous venons de signaler.

Les indicateurs de cycles, auxquels nous avons fait allusion plus haut, semblent avoir peu retenu l'attention des géomètres, jusqu'à ces derniers temps. Sauf erreur, aucun des ouvrages classiques de Serret, Jordan, Netto, Burnside ou Speiser, sur la théorie des groupes ou des substitutions, n'en fait mention et ils ne figurent pas d'avantage dans les traités d'analyse combinatoire de Netto ou de Mac-Mahon. Il y a longtemps, cependant, qu'une expression de ce genre, celle qui est relative au groupe symétrique tout entier, a été donnée explicitement par Cauchy, mais, à notre connaissance du moins, l'appel systématique aux fonctions indicatrices de cycles a été fait par M. J. Schur[1], qui les nomme »Hauptcharakteristik». Récemment, dans un beau mémoire sur les arbres de Cayley et sur les combinaisons de la chimie organique, M. G. Pólya[2] s'en est servi, sous le nom de »Zyklenzeiger», en liaison avec certains groupes spéciaux, comme le groupe de

[1] J. SCHUR. — Darstellungstheorie der Gruppen. Zürich, 1936, pages 59 et 68.

[2] G. PÓLYA. — Act. Math. T. 68 — 1937 — page 122. — voir également, dans un cas particulier, Pólya et Szegö — Aufgaben und Lehrsätze aus der Analysis. — Bd II, p. 311.

l'octaèdre. Ayant, de notre côté, rencontré ces fonctions dans nos recherches sur les cycles primaires et secondaires des substitutions, sous une forme plus générale que les deux éminents auteurs cités et en poursuivant un but bien différent du leur, ce que nous en dirons ici ne risquera pas de faire double emploi avec les résultats de leurs travaux.

§ I.

Propriétés des cycles primaires.

1. Soit A une propriété que nous attribuerons à certains cycles ou à tous les cycles d'une substitution. Cette propriété devra satisfaire essentiellement à la condition suivante: Si, avec une certaine combinaison de p lettres, $u_1, u_2, \ldots u_p$, $(p = 1, 2, 3, \ldots n)$, prises parmi les n lettres données, $u_1, u_2, \ldots u_n$, on peut former un nombre a_p de substitutions circulaires d'ordre p, jouissant de la propriété A, avec toute autre combinaison de p lettres, $u'_1, u'_2, \ldots u'_p$, prises parmi les n lettres données, on pourra former exactement le même nombre a_p de substitutions circulaires d'ordre p, jouissant de la propriété A. Aucune combinaison de p lettres, $(p = 1, 2, 3, \ldots n)$, n'est privilégiée; il y a égale répartition de la propriété A entre toutes les combinaisons d'un même nombre de lettres.

Une telle propriété A peut être définie de bien des manières; les cycles pourront, par exemple, être d'un ordre déterminé, ou bien d'un ordre quelconque, sauf certains ordres déterminés; ou bien encore, si on les représente géométriquement par des polygônes inscrits dans une circonférence, les cycles pourront affecter telle ou telle figure. Mais la façon la plus générale de concevoir une propriété A est de dresser un tableau des substitutions circulaires qui seront censées la posséder, tableau d'ailleurs arbitraire, pourvu qu'il satisfasse à la condition essentielle que nous avons énoncée. Les nombres entiers, $a_1, a_2, a_3, \ldots$ seront tels que $0 \leq a_i \leq (i-1)!$, $(i = 1, 2, 3, \ldots)$; la fonction

$$a(z) = a_1 \frac{z}{1} + a_2 \frac{z^2}{2!} + a_3 \frac{z^3}{3!} + \cdots$$

sera majorée par la série $-\log(1-z)$ et nous l'appellerons, pour abréger, une fonction génératrice de cycles. Au-contraire, une fonction

$$u_0 + u_1 \frac{z}{1} + u_2 \frac{z^2}{2!} + \cdots$$

où les entiers u_i sont tels que $0 \leq u_i \leq i!$, $(i = 1, 2, 3, \ldots)$ sera majorée par la série $(1 - z)^{-1}$ et nous l'appellerons une fonction génératrice de substitutions.

Si l'on a affaire à plusieurs propriétés A, B ou C, nous supposerons, sauf avis contraire expressément formulé, que ces propriétés s'excluent mutuellement; les cycles qui possèdent l'une d'elles devront être distincts des cycles qui en possèdent une autre, de sorte que $b(z)$ et $c(z)$ désignant les fonctions génératrices de cycles, analogues à $a(z)$, non seulement chacune des séries $a(z)$, $b(z)$, $c(z)$, sera majorée par la série $-\log(1-z)$, mais encore leur somme, $a(z) + b(z) + c(z)$, sera également majorée par la même série $-\log(1-z)$.

Enfin, il nous arrivera, pour alléger notre texte, d'écrire qu'un cycle est un cycle A, ou même qu'un cycle est A, pour exprimer que ce cycle possède la propriété A.

2. Cela étant, cherchons d'abord le nombre P_n des substitutions de n lettres, dont tous les cycles sont A. Supposons connus $P_1, P_2, \ldots P_n$, et aux n lettres $u_1, u_2, \ldots u_n$, ajoutons une $(n+1)^{\text{ème}}$ lettre pour calculer P_{n+1}. Cette lettre u_{n+1} peut entrer dans un cycle d'ordre $1, 2, 3, \ldots$ ou $n+1$. Si elle figure dans un cycle d'ordre $p+1$, il y a $\binom{n}{p}$ manières de l'associer à une combinaison p à p des n premières lettres; on a ainsi une combinaison de $p+1$ lettres qui donne naissance à a_{p+1} cycles, jouissant de la propriété A. Chacun de ces cycles doit être facteur d'une substitution partielle des $n-p$ lettres non utilisées. Dans ces substitutions partielles, tous les cycles doivent posséder la propriété A; leur nombre est donc P_{n-p}, d'où le terme $\binom{n}{p} a_{p+1} P_{n-p}$ et la formule récurrente qui en découle,

$$P_{n+1} = a_1 P_n + \cdots + \binom{n}{p} a_{p+1} P_{n-p} + \cdots + a_{n+1} P_0. \tag{1}$$

Le dernier terme à droite est relatif aux substitutions circulaires de $n+1$ lettres; elles sont au nombre de a_{n+1}; il faut donc faire conventionellement $P_0 = 1$. Soit alors

$$P(z) = \sum_{n=0}^{\infty} P_n \frac{z^n}{n!}$$

la fonction génératrice des nombres P_n, il résulte de (1) que

$$P'(z) = a(z) P(z),$$

$P'(z)$ désignant la dérivée de $P(z)$, d'où, en intégrant,

$$P(z) = \sum_{n=0}^{\infty} P_n \frac{z^n}{n!} = e^{a(z)}. \tag{2}$$

Les indicateurs de cycles des ensembles de substitutions du groupe symétrique, dont tous les cycles sont A, se calculent de proche en proche, grâce à l'équation (1),

$$\left\{\begin{aligned}
P_0 &= 1\\
P_1 &= a_1\\
P_2 &= a_1^2 + a_2\\
P_3 &= a_1^3 + 3\,a_1 a_2 + a_3\\
P_4 &= a_1^4 + 6\,a_1^2 a_2 + 4\,a_1 a_3 + 3\,a_2^2 + a_4\\
P_5 &= a_1^5 + 10\,a_1^3 a_2 + 10\,a_1^2 a_3 + 15\,a_1 a_2^2 + 5\,a_1 a_4 + 10\,a_2 a_3 + a_5\\
P_6 &= a_1^6 + 15\,a_1^4 a_2 + 20\,a_1^3 a_3 + 45\,a_1^2 a_2^2 + 15\,a_1^2 a_4 + 6\,a_1 a_5 + 60\,a_1 a_2 a_3\\
&\quad + 15\,a_2^3 + 15\,a_2 a_4 + 10\,a_3^2 + a_6\\
P_7 &= a_1^7 + 21\,a_1^5 a_2 + 35\,a_1^4 a_3 + 105\,a_1^3 a_2^2 + 35\,a_1^3 a_4 + 210\,a_1^2 a_2 a_3 + 21\,a_1^2 a_5\\
&\quad + 105\,a_1 a_2^3 + 105\,a_1 a_2 a_4 + 70\,a_1 a_3^2 + 7\,a_1 a_6 + 105\,a_2^2 a_3 + 21\,a_2 a_5\\
&\quad + 35\,a_3 a_4 + a_7\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned}\right. \tag{3}$$

L'expression générale des fonctions P_i s'obtient en développant l'exponentielle de la formule (2)

$$\frac{P_n}{n!} = \sum \frac{1}{\alpha_1!\,\alpha_2!\dots\alpha_n!}\left(\frac{a_1}{1}\right)^{\alpha_1}\left(\frac{a_2}{2!}\right)^{\alpha_2}\dots\left(\frac{a_n}{n!}\right)^{\alpha_n}, \tag{4}$$

où

$$\alpha_1 + 2\,\alpha_2 + 3\,\alpha_3 + \cdots + n\alpha_n = n.$$

Si la propriété A, attribuable aux cycles, consiste à être une substitution circulaire quelconque, on devra, dans les expressions (3) et (4), faire $a_\nu = (\nu - 1)!$, ou mieux $a_\nu = (\nu - 1)!\,x_\nu$, x_ν désignant une variable d'ordre, c'est-à-dire une variable sans valeur numérique, dont l'indice ν, $(\nu = 1, 2, 3, \dots)$, spécifie l'ordre des cycles auxquels elle se rapporte. Les fonctions (3) se réduisent alors aux caractéristiques principales de M. J. Schur et l'équation (4) devient celle qu'a donnée Cauchy. Dans le cas général, on tire immédiatement de (4) la solution du problème suivant: Parmi toutes les substitutions sembables à une substitution donnée, déterminer le nombre de celles dont tous les cycles jouissent d'une propriété A. Il est clair que l'équation (4) n'est autre que l'une des formules, données par

Waring, pour le calcul des fonctions symétriques des racines d'une équation et il serait facile, comme le fait M. Schur, dans son ouvrage cité, de rattacher les polynômes P_n aux fonctions de H. Wronski.

3. Pour donner un exemple d'application de ce qui précède, supposons que les cycles aient la propriété d'être représentés géométriquement par des polygônes réguliers convexes, inscrits dans une circonférence et parcourus dans un sens déterminé; il y aura alors, pour chaque combinaison de chaque ordre, un seul cycle répondant à la question, de sorte que $a_1 = a_2 = a_3 = \cdots = 1$ et que

$$a(z) = e^z - 1 .$$

La fonction génératrice des nombres P_n est donc, dans ce cas,

$$P(z) = e^{e^z - 1}$$

et l'équation (4) donne l'expression des coefficients du développement de Taylor de cette double exponentielle.

Comme autre exemple, supposons que tous les cycles doivent être d'ordre carré parfait. On aura

$$a(q) = \int_0^q \frac{\vartheta_3(0) - 1}{2q}\, dq$$

où

$$\vartheta_3(0) = 1 + 2q + 2q^4 + 2q^9 + \cdots .$$

Or, Jacobi[1] a donné une équation différentielle algébrique du troisième ordre, à laquelle satisfait ϑ_3. Il serait donc aisé d'obtenir une équation différentielle du quatrième ordre, pour la fonction génératrice

$$e^{a(q)} = \sum_{n=0}^{\infty} P_n \frac{q^n}{n!}$$

et, d'autre part, l'équation (4) donne l'expression explicite des nombres P_n, si l'on y fait a_ν égal à $(\nu - 1)!$ ou à zéro, suivant que ν est ou n'est pas carré parfait.

4. Je cherche maintenant le nombre $P_n^{\lambda, \mu, \nu}$ des substitutions de n lettres, dont λ cycles exactement sont A, dont μ cycles exactement sont B, dont ν cycles exactement sont C et dont tous les autres cycles sont D. Une telle substitution

[1] Voir, par exemple, HURWITZ — Oeuvres — Bd I, p. 294.

ne peut exister que si elle contient, au moins, $\lambda + \mu + \nu$ cycles; $P_n^{\lambda,\mu,\nu}$ est donc nécessairement nul, quelles que soient les propriétés A, B, C, D, tant que l'indice n est inférieur à $\lambda + \mu + \nu$.

Raisonnons comme plus haut, en adjoignant une nouvelle lettre u_{n+1} aux n lettres $u_1, u_2, \ldots u_n$ et en calculant $P_{n+1}^{\lambda,\mu,\nu}$. Supposons que u_{n+1} figure dans un cycle d'ordre $p+1$. Ce cycle peut avoir la propriété A; il faut alors l'associer aux substitutions partielles dénombrées par $P_{n-p}^{\lambda-1,\mu,\nu}$, d'où le terme $\binom{n}{p} a_{p+1} P_{n-p}^{\lambda-1,\mu,\nu}$; ou bien, il a la propriété B, d'où le terme $\binom{n}{p} b_{p+1} P_{n-p}^{\lambda,\mu-1,\nu}$; ou bien, il a la propriété C, d'où le terme $\binom{n}{p} c_{p+1} P_{n-p}^{\lambda,\mu,\nu-1}$; ou, enfin, il a la propriété D, d'où le terme $\binom{n}{p} d_{p+1} P_{n-p}^{\lambda,\mu,\nu}$. On a donc, en faisant successivement $p = 0, 1, 2, \ldots$

$$P_{n+1}^{\lambda,\mu,\nu} = \sum_{p=0}^{n} \binom{n}{p} \left[a_{p+1} P_{n-p}^{\lambda-1,\mu,\nu} + b_{p+1} P_{n-p}^{\lambda,\mu-1,\nu} + c_{p+1} P_{n-p}^{\lambda,\mu,\nu-1} + d_{p+1} P_{n-p}^{\lambda,\mu,\nu}\right],$$

ou, sous forme symbolique,

$$(5)\quad P_{n+1}^{\lambda,\mu,\nu} = a(a + P^{\lambda-1,\mu,\nu})^n + b(b + P^{\lambda,\mu-1,\nu})^n + c(c + P^{\lambda,\mu,\nu-1})^n + d(d + P^{\lambda,\mu,\nu})^n.$$

D'ailleurs, on doit prendre $P_0^{\lambda,\mu,\nu} = 0$, car il n'existe aucune substitution circulaire répondant à la question. Il résulte visiblement de la formule (5) que $a(z)$, $b(z)$, $c(z)$, $d(z)$ désignant les fonctions génératrices des cycles correspondant respectivement aux propriétés A, B, C, D, la fonction génératrice de substitutions

$$f_{\lambda,\mu,\nu}(z) = \sum_{n=0}^{\infty} P_n^{\lambda,\mu,\nu} \frac{z^n}{n!}$$

satisfait à la relation

$$f'_{\lambda,\mu,\nu}(z) = a'(z) f_{\lambda-1,\mu,\nu}(z) + b'(z) f_{\lambda,\mu-1,\nu}(z) + c'(z) f_{\lambda,\mu,\nu-1}(z) + d'(z) f_{\lambda,\mu,\nu}(z),$$

dont l'intégrale, répondant aux conditions initiales que nous avons posées, est

$$(6)\qquad f_{\lambda,\mu,\nu}(z) = \frac{a^\lambda(z)}{\lambda!} \frac{b^\mu(z)}{\mu!} \frac{c^\nu(z)}{\nu!} e^{d(z)}.$$

A l'aide de l'équation (5), il serait possible de calculer de proche en proche les indicateurs de cycles des substitutions étudiées et l'équation (6) permettrait d'en former l'expression générale. Bornons-nous au cas simple suivant; soit

$$S = \Gamma_1^{\beta_1} \Gamma_2^{\beta_2} \cdots \Gamma_i^{\beta_i} C_1^{\alpha_1} C_2^{\alpha_2} \cdots C_j^{\alpha_j},$$

$$\beta_1 + \beta_2 + \cdots + \beta_i = \lambda,$$

$$\beta_1 + 2\beta_2 + \cdots + i\beta_i + \alpha_1 + 2\alpha_2 + \cdots + j\alpha_j = n,$$

une substitution dont les λ cycles Γ_ν, d'ordre ν, $(\nu = 1, 2, 3, \ldots i)$, possèdent la propriété B et dont les cycles restants C_ν, d'ordre ν, $(\nu = 1, 2, 3, \ldots j)$, possèdent la propriété A. Le nombre des substitutions, semblables à S, dont λ cycles exactement possèdent la propriété B et dont tous les autres cycles possèdent la propriété A, est égal à

$$\frac{n!}{\beta_1! \ldots \beta_i! \, \alpha_1! \ldots \alpha_j!} \left(\frac{b_1}{1}\right)^{\beta_1} \cdots \left(\frac{b_i}{i!}\right)^{\beta_i} \left(\frac{a_1}{1}\right)^{\alpha_1} \cdots \left(\frac{a_j}{j!}\right)^{\alpha_j},$$

ce qui constitue une généralisation de la formule (4).

5. Voici maintenant une conséquence de l'équation (6), lorsqu'on y fait $\nu = 0$ et qu'on y remplace $d(z)$ par $c(z)$.

Le nombre R_n des substitutions de n lettres, qui contiennent autant de cycles A que de cycles B et dont tous les cycles restants sont des cycles C, est évidemment

$$R_n = P_n^{0,0} + P_n^{1,1} + \cdots + P_n^{k,k} + \cdots.$$

Or, d'après (6), $P_n^{k,k}$ est le résidu à l'origine de

$$n! \frac{e^{c(z)}}{z^{n+1}} \frac{a^k(z)\, b^k(z)}{k!\, k!},$$

donc, en employant le symbole $\mathcal{E}$ des résidus de Cauchy,

$$R_n = n! \mathop{\mathcal{E}} \frac{e^{c(z)}}{z^{n+1}} \left[1 + \frac{a(z)\, b(z)}{(1!)^2} + \frac{a^2(z)\, b^2(z)}{(2!)^2} + \cdots \right],$$

où l'on observera que la série entre crochets peut être prolongée indéfiniment puisque, $a(z)$ et $b(z)$ n'ayant pas de terme constant, les résidus s'annulent d'eux-mêmes, à partir d'un certain rang. On a donc

$$\sum_{n=0}^{\infty} R_n \frac{z^n}{n!} = e^{c(z)} J_0\left(2i\sqrt{a(z)\, b(z)}\right)$$

où

$$J_0(2i\sqrt{x}) = 1 + \frac{x}{(1!)^2} + \frac{x^2}{(2!)^2} + \cdots$$

est la fonction bien connue de Bessel.

Si, en particulier, la propriété A consiste à être d'ordre p, si la propriété B consiste à être d'ordre q et si la propriété C consiste à n'être ni d'ordre p, ni d'ordre q, propriétés qui s'excluent mutuellement, comme cela doit être, on aura

$$a(z) = \frac{z^p}{p}, \quad b(z) = \frac{z^q}{q}, \quad c(z) = \log\frac{1}{1-z} - \frac{z^p}{p} - \frac{z^q}{q}$$

et

$$\sum_{n=0}^{\infty} R_n \frac{z^n}{n!} = \frac{1}{1-z} e^{-\frac{z^p}{p} - \frac{z^q}{q}} J_0\left(\frac{2i}{\sqrt{pq}} z^{\frac{p+q}{2}}\right),$$

d'où l'on pourrait déduire l'expression[1] exacte et l'expression asymptotique des nombres R_n.

On prouverait, plus généralement que le nombre R_n^h des substitutions de n lettres, dans lesquelles le nombre des cycles B surpasse de h unités le nombre des cycles A, h étant fixe, indépendant de n, et dont tous les autres cycles possèdent la propriété C, a pour fonction génératrice

$$\sum_{n=0}^{\infty} R_n^h \frac{z^n}{n!} = e^{-\frac{\pi h i}{2}} \left[\frac{b(z)}{a(z)}\right]^{\frac{h}{2}} e^{c(z)} J_h\left[2i\sqrt{a(z)\,b(z)}\right],$$

$J_h(x)$ étant la fonction de Bessel de première espèce, d'indice h.

Une généralisation immédiate de la question mettrait en jeu les fonctions de Bessel d'ordre supérieur, étudiées notamment par M. Pierre Humbert[2] et qui se déduisent par confluence de séries hypergéométriques.

6. Cherchons encore le nombre S_n des substitutions carrées de n lettres, dont tous les cycles possèdent une propriété A, en entendant par substitutions carrées celles qui sont les secondes puissances d'une autre substitution.

Une substitution est un carré, lorsqu'elle contient des cycles d'ordre impair en nombre quelconque et des couples de cycles d'un même ordre, quand cet ordre est pair. Le nombre S_n se calcule alors, en modifiant légèrement le raisonnement déjà utilisé deux fois, au moyen de la formule récurrente

---

[1] Ann. de la Soc. Scient. de Bruxelles — 1933 — p. 126.

[2] P. HUMBERT — Atti della Pont. Acc. Nuovi Lincei — 1930 — page 130.

$$(7) \qquad S_{n+1} = a_1 S_n + \binom{n}{2} a_3 S_{n-2} + \binom{n}{4} a_5 S_{n-4} + \cdots$$
$$+ \binom{n}{1}\binom{n-1}{2} a_2^2 S_{n-3} + \binom{n}{3}\binom{n-3}{4} a_4^2 S_{n-7} + \binom{n}{5}\binom{n-5}{6} a_6^2 S_{n-11} + \cdots$$

qui donne successivement les indicateurs de cycles

$$S_0 = 1$$
$$S_1 = a_1$$
$$S_2 = a_1^2$$
$$S_3 = a_1^3 + a_3$$
$$S_4 = a_1^4 + 4\, a_1 a_3 + 3\, a_2^2$$
$$S_5 = a_1^5 + 10\, a_1^2 a_3 + 15\, a_1 a_2^2 + a_5$$
$$S_6 = a_1^6 + 20\, a_1^3 a_3 + 45\, a_1^2 a_2^2 + 6\, a_1 a_5 + 10\, a_3^2$$
$$S_7 = a_1^7 + 35\, a_1^4 a_3 + 105\, a_1^3 a_2^2 + 21\, a_1^2 a_5 + 70\, a_1 a_3^2 + 105\, a_2^2 a_3 + a_7$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

et ces expressions sont conformes à celles qui se déduiraient du tableau (3).

Quant à la fonction génératrice

$$S(z) = \sum_{n=0}^{\infty} S_n \frac{z^n}{n!},$$

il est nécessaire, pour l'exprimer simplement, de faire appel non seulement à la série habituelle

$$a(z) = a_1 \frac{z}{1!} + a_2 \frac{z^2}{2!} + \cdots$$

mais encore à la série

$$u(z) = \frac{a_2^2}{1!\,2!} z^3 + \frac{a_4^2}{3!\,4!} z^7 + \frac{a_6^2}{5!\,6!} z^{11} + \cdots .$$

On déduit alors de (7) que

$$\log S(z) = \frac{a(z) - a(-z)}{2} + \int_0^z u(z)\, dz$$

et on peut observer, qu'à l'aide du théorème de Parseval, on a

$$\int_0^z u(z)\,dz = \frac{1}{8\pi i}\int_\gamma a(u)\left[a\left(\frac{z^2}{u}\right) - a\left(-\frac{z^2}{u}\right)\right]\frac{du}{u},$$

γ étant un contour suffisamment petit, entourant le point $u = 0$, dans le plan de la variable u.

En particulier, pour $a_\nu = (\nu - 1)!$, $(\nu = 1, 2, 3, \ldots)$, le nombre σ_n des substitutions carrées de n lettres a pour fonction génératrice $\sigma(z)$, où

$$\log \sigma(z) = \frac{1}{2}\log\frac{1+z}{1-z} - \frac{1}{2}\int_0^z \log(1 - z^4)\frac{dz}{z}.$$

La considération des substitutions cubes conduirait à des résultats analogues, mais un problème bien plus intéressant consisterait à étendre les résultats du présent paragraphe à des substitutions prises successivement dans une suite de groupes d'ordres croissants, à définir convenablement et non plus dans la suite banale des groupes symétriques de degrés successifs $1, 2, 3, \ldots$. En dehors des groupes intransitifs qu'on obtient par la réunion de deux ou plusieurs groupes symétriques, permutant des systèmes de lettres différents, et qui présentent peu d'intérêt, de telles suites de groupes, paraissant susceptibles de donner naissance à un calcul régulier abordable, sont fort rares. Tels seraient cependant les groupes d'ordre $n!$ et de degré $\binom{n}{k}$, k fixe, $n = k, k+1, k+2, \ldots$ qui permutent les combinaisons k à k de n lettres et qui sont holoédriquement isomorphes au groupe symétrique de ces mêmes lettres. Tels seraient encore certains groupes abéliens, d'ordre p^m, p étant un nombre premier fixe, $m = 1, 2, 3, \ldots$ et de type $(1, 1, 1, \ldots 1)$ et les groupes de leurs isomorphismes. Nous n'examinerons, plus loin, la question que dans le cas très simple du groupe alterné.

§ II.

Sur certains polynomes.

7. Soient $a(z)$, $b(z)$, $c(z)$ des fonctions génératrices de cycles, relatives à des propriétés A, B, C, qui s'excluent mutuellement et considérons le développement

$$e^{a(z) + x b(z) + y c(z)} = \sum_{n=0}^{\infty} \chi_n(x, y)\frac{z^n}{n!}.$$

Les séries $a(z)$, $b(z)$ et $c(z)$ n'ayant pas de termes constants, $\chi_n(x, y)$ est un polynôme de degré n au plus. Si l'on développe l'exponentielle du premier membre, le coefficient de $x^\lambda y^\mu$ est

$$\frac{c^\mu(z)}{\mu!}\frac{b^\lambda(z)}{\lambda!}e^{a(z)},$$

expression qui est de la même forme que (6), au § I et dans le développement de laquelle nous savons interpréter le coefficient de $\frac{z^n}{n!}$, comme dénombrant certaines substitutions. Par suite, dans le polynôme $\chi_n(x, y)$, le terme en $x^\lambda y^\mu$ est le nombre des substitutions de n lettres dont λ cycles exactement sont B, dont μ cycles exactement sont C et dont tous les autres cycles sont A.

Soit maintenant

$$\frac{[b(z)]^\lambda}{\lambda!}e^{x\,a(z)} = \sum_{n=0}^{\infty} P_n(x)\frac{z^n}{n!};$$

$P_n(x)$ est un polynôme de degré $n-\lambda$ au plus et un raisonnement analogue à celui qui vient d'être fait montre que ce polynôme dénombre les substitutions Σ_n de n lettres, dont λ cycles, λ fixe, jouissent de la propriété B et dont tous les autres cycles jouissent de la propriété A. Dans $P_n(x)$, le coefficient de x^μ est le nombre de ces substitutions Σ_n qui sont décomposables en $\lambda+\mu$ cycles exactement.

Si l'on fait notamment $a(z)=z$, c'est-à-dire $a_1=1$, $a_2=a_3=\cdots=0$, la propriété A consiste à n'échanger aucune lettre et les polynômes d'Appell, dérivés de la fonction génératrice

$$\frac{b^\lambda(z)}{\lambda!}e^{xz} = \sum_{n=0}^{\infty} P_n(x)\frac{z^n}{n!}, \tag{8}$$

dénombrent les substitutions de n lettres qui n'échangent que celles contenues dans λ cycles, jouissant tous de la propriété B. Il nous semble intéressant de rappeler, à ce sujet, qu'Appell avait défini des opérations linéaires permutables, permettant de passer des fonctions génératrices $a(z)e^{xz}$ et $b(z)e^{xz}$ à la fonction génératrice $a(z)b(z)e^{xz}$ et, par suite, de $a(z)e^{xz}$ à $a^\lambda(z)e^{xz}$, λ étant un exposant entier et positif quelconque.

8. Soit, en particulier, $H_n(x)$ un polynôme d'Hermite et soit $\bar{\omega}_n(x) = i^n H_n(-xi)$; on a

$$e^{\frac{z^2}{2}+xz} = \sum_{n=0}^{\infty} \bar{\omega}_n(x)\frac{z^n}{n!};$$

or, dans le développement de

$$\frac{z^k}{k!}e^{\frac{z^2}{2}},$$

le coefficient de $\frac{z^n}{n!}$ est, en vertu de (6), égal au nombre des substitutions de n lettres, dont k cycles sont des cycles unités et dont tous les autres cycles sont d'ordre 2. $\bar{\omega}_n(x)$ dénombre donc toutes les substitutions d'ordre 1 ou 2, c'est-à-dire toutes les racines carrées de la substitution identique E, y compris la substitution identique E, elle-même. Le coefficient de x^μ dans $\bar{\omega}_n(x)$ est le nombre de ces racines carrées qui laissent μ lettres inchangées. Les racines primitives de E, c'est-à-dire E étant exclue, sont dénombrées par le polynôme $\chi_n(x) = \bar{\omega}_n(x) - x^n$ et l'on a immédiatement, x_1 et x_2 étant deux nouvelles variables,

$$e^{x_1 z + x_2 \frac{z^2}{2}} - e^{x_1 z} = \sum_{n=0}^{\infty} x_2^{\frac{n}{2}} \chi_n\left(\frac{x_1}{\sqrt{x_2}}\right)\frac{z^n}{n!} = \sum_{n=0}^{\infty} \chi_n(x_1, x_2)\frac{z^n}{n!}.$$

On voit ainsi que le polynôme $\chi_n(x_1, x_2)$ non seulement dénombre les racines carrées primitives de E, mais qu'il les représente, en ce sens que c'est un indicateur de cycles de ces substitutions.

On peut généraliser cette formule. Soient p et q deux nombres premiers; les racines primitives de l'équation binôme $u^{pq} - 1 = 0$ sont les racines de

$$\frac{(u^{pq}-1)(u-1)}{(u^p-1)(u^q-1)} = 0.$$

D'une manière analogue, le polynôme χ_n, à quatre variables, engendré par

$$e^{x_1 z + x_p \frac{z^p}{p} + x_q \frac{z^q}{q} + x_{pq}\frac{z^{pq}}{pq}} - e^{x_1 z + x_p \frac{z^p}{p}} - e^{x_1 z + x_q \frac{z^q}{q}} + e^{x_1 z} = \sum_{n=0}^{\infty} \chi_n(x_1, x_p, x_q, x_{pq})\frac{z^n}{n!}$$

est l'indicateur de cycles des racines primitives d'ordre pq de la substitution identique et il serait facile, en se fondant sur la théorie des équations binômes, d'étendre ce résultat aux racines primitives de E, d'ordre m, m étant un entier positif quelconque.

9. Pour donner une autre interprétation du polynôme $\chi_n(x)$, convenons, par analogie avec la théorie des permutations rectilignes[1], d'appeler substitutions circulaires auto-conjuguées d'ordre impair, $2k+1$, les substitutions circulaires

[1] E. Netto. — Lehrbuch der Combinatorik — 2e Ed. — 1927 — page 90.

dans lesquelles la lettre u_α occupe la place γ, différente de α, et la lettre u_γ occupe la place α, exception faite pour la seule lettre u_1, qui occupe la place 1. Le nombre β_{2k+1} de ces substitutions circulaires, relatives à $2k+1$ lettres, est égal à $1.3.5\ldots(2k-1)$ et le nombre β_{2k} est nul. Appelons de même substitutions circulaires auto-conjuguées d'ordre pair, $2k$, les substitutions circulaires dans lesquelles deux lettres sont à leur place, d'abord u_1, puis une lettre variable, qui sera successivement $u_2, u_3 \ldots$ et u_{2k}, les $2k-2$ lettres restantes étant conjuguées deux à deux, comme il vient d'être dit. Le nombre b_{2k} des substitutions auto-conjuguées, d'ordre $2k$, est $1.3.5\ldots(2k-1)$ et le nombre b_{2k+1} est nul.

Ces définitions posées, observons que la série $e^{\frac{z^2}{2}}-1$ est majorée par la série $-\log(1-z)$ et peut, par suite, être considérée comme une fonction génératrice de cycles,

$$b(z) = e^{\frac{z^2}{2}-1} = b_2\frac{z^2}{2!} + b_4\frac{z^4}{4!} + b_6\frac{z^6}{6!} + \cdots,$$

où b_{2k} a la valeur indiquée ci-dessus. L'équation

$$\left(e^{\frac{z^2}{2}} - 1\right) e^{xz} = \sum_{n=0}^{\infty} \chi_n(x)\frac{z^n}{n!} \tag{9}$$

rentre donc dans la formule (8), pour $\lambda = 1$, et le polynôme $\chi_n(x)$ dénombre les substitutions T_n, de n lettres, dont un cycle est auto-conjugué d'ordre pair et dont tous les autres cycles sont des cycles unités. Le coefficient de x^μ, dans $\chi_n(x)$, est égal au nombre de ces substitutions T_n qui contiennent, en plus du cycle auto-conjugué, μ cycles d'ordre 1.

Soit maintenant

$$R_n(x_1, y) = y^n \chi_n\left(\frac{x_1}{y}\right);$$

on a, d'après (9),

$$e^{x_1 z + \frac{1}{2}y^2 z^2} - e^{x_1 z} = \sum_{n=0}^{\infty} R_n(x_1, y)\frac{z^n}{n!};$$

dans $R_n(x_1, y)$, considérons les exposants de la variable y comme des indices, c'est-à-dire remplaçons $y^{2\mu}$ par $y_{2\mu}$; le polynôme obtenu, linéaire en $y_2, y_4, y_6, \ldots$ est alors un indicateur de cycles pour les substitutions T_n, le cycle auto-conjugué ayant pour symbole la variable y et les cycles unités ayant pour symbole la variable x_1.

10. Nous venons d'obtenir deux interprétations distinctes des polynômes $\chi_n(x)$, dérivés des polynômes d'Hermite. Plus généralement, considérons la fonction

$$(10) \qquad y(z) = e^{x\,a(z)+b(z)} = \sum_{n=0}^{\infty} P_n(x)\frac{z^n}{n!};$$

nous savons, d'une part, que, dans $P_n(x)$, le coefficient de x^μ est égal au nombre des substitutions de n lettres, dont μ cycles sont A et dont tous les autres cycles sont B. Supposons, d'autre part, que la série, développant $e^{b(z)} - 1$, soit majorée par $-\log(1-z)$ et soit

$$\beta(z) = e^{b(z)} - 1 = \sum_{n=0}^{\infty} \beta_n \frac{z^n}{n!}.$$

Aux nombres $\beta_1, \beta_2, \beta_3, \ldots$ correspond un certain tableau de cycles et, par conséquent, une certaine propriété β de ces cycles et, si l'on développe

$$u(z) = \beta(z)\,e^{x\,a(z)} = \sum_{0}^{\infty} Q_n(x)\frac{z^n}{n!},$$

le coefficient de x^μ, dans $Q_n(x)$, est égal au nombre des substitutions de n lettres, décomposables en $\mu + 1$ cycles exactement, dont l'un jouit de la propriété β et dont les μ autres jouissent de la propriété A.

Enfin, soit

$$v(z) = e^{x\,a(z)} = \sum_{n=0}^{\infty} R_n(x)\frac{z_n}{n!};$$

le coefficient de x^μ, dans $R_n(x)$, est égal au nombre des substitutions de n lettres, décomposables en μ cycles exactement, ces cycles jouissant tous de la propriété A.

En comparant les trois fonctions $y(z)$, $u(z)$, $v(z)$, on voit que $y(z) = u(z) + v(z)$. Cette relation qui, dans le cas particulier des polynômes $\chi_n(x)$, nous a fourni leur double interprétation, contient, dans le cas général une proposition qu'il serait facile d'énoncer.

11. Arrêtons-nous actuellement sur le cas où, parmi les cycles d'une substitution, on distingue celui qui contient une lettre donnée, la première lettre u_1, par exemple. Soit $Q_n^{\lambda+1}$ le nombre des substitutions de n lettres, décomposables en $\lambda + 1$ cycles exactement, dont l'un, celui qui contient la lettre u_1, est un

cycle B et dont les λ autres sont des cycles A. Nous avons ici, contrairement à la condition posée au § I, des combinaisons privilégiées, celles qui contiennent la lettre u_1, mais cette condition subsiste entièrement pour les lettres non désignées et il suffit de conduire le calcul différemment, en mettant à part la lettre distinguée u_1, pour parvenir à l'équation récurrente suivante

$$Q_{n+1}^{\lambda+1} = a_1 Q_n^\lambda + \binom{n-1}{1} a_2 Q_{n-1}^\lambda + \binom{n-1}{2} a_3 Q_{n-2}^\lambda + \cdots$$

$$+ b_2 P_{n-1}^\lambda + \binom{n-1}{1} b_3 P_{n-2}^\lambda + \binom{n-1}{2} b_4 P_{n-3}^\lambda + \cdots,$$

où j'ai désigné par P_ν^λ le nombre des substitutions de ν lettres, décomposables en λ cycles exactement, jouissant de la propriété A, nombre figurant dans le développement

$$\frac{a^\lambda(z)}{\lambda!} = P_0^\lambda + P_1^\lambda \frac{z}{1} + \cdots + P_{n-1}^\lambda \frac{z^{n-1}}{(n-1)!} + \cdots.$$

On en déduit, pour la fonction génératrice

$$\varphi_{\lambda+1}(z) = Q_1^{\lambda+1} + \cdots + Q_{n+1}^{\lambda+1} \frac{z^n}{n!} + \cdots = \sum_{n=1}^{\infty} Q_n^{\lambda+1} \frac{z^{n-1}}{(n-1)!},$$

la relation

$$\varphi'_{\lambda+1}(z) = a'(z)\varphi_\lambda(z) + b''(z)\frac{a^\lambda(z)}{\lambda!},$$

dont l'intégrale, satisfaisant aux conditions initiales

$$Q_1^{\lambda+1} = Q_2^{\lambda+1} = \cdots = Q_\lambda^{\lambda+1} = 0,$$

$$Q_{\lambda+1}^{\lambda+1} = b_1 a_1^\lambda = 1,$$

est

$$\varphi_{\lambda+1}(z) = b'(z)\frac{a^\lambda(z)}{\lambda!}, \qquad \varphi_0(z) = 0;$$

ce point acquis, posons

$$b'(z)\, e^{x a(z)} = \sum_{n=1}^{\infty} B_n(x) \frac{z^{n-1}}{(n-1)!}; \tag{11}$$

comme nous l'avons fait précédemment, nous développerons en série l'exponentielle et nous verrons que le coefficient de x^μ, dans le polynôme $B_n(x)$, est le nombre des substitutions de n lettres, décomposables en $\mu + 1$ cycles exactement, dont l'un, celui qui contient la lettre u_1, jouit de la propriété B et dont les μ autres jouissent de la propriété A. L'intérêt de la formule (11) réside en ce que la série $b(z)$ étant majorée par $-\log(1-z)$, sa dérivée $b'(z)$ est majorée moins étroitement par la série $(1-z)^{-1}$ et peut, par suite, être considérée comme une fonction génératrice de substitutions.

Si l'on considère alors l'équation (10) et si l'on pose

$$\beta'(z) = e^{b(z)},$$

cette équation devient

$$\beta'(z)\, e^{x\,a(z)} = \sum_0^\infty P_n(x) \frac{z^n}{n!}. \tag{12}$$

Aux nombres $\beta_1, \beta_2, \beta_3, \ldots$ correspond une certaine propriété β des substitutions circulaires et le coefficient de x^μ, dans $P_n(x)$, est, d'après (11), le nombre des substitutions de $n+1$ lettres, décomposables en $\mu+1$ cycles exactement, dont l'un, celui qui contient la lettre u_1, jouit de la propriété β et dont les μ autres jouissent de la propriété A. On peut donc énoncer le théorème suivant: s'il y a autant de substitutions circulaires de $n+1$ lettres, jouissant de la propriété β, que de substitutions de n lettres, dont les cycles jouissent de la propriété B, alors le nombre des substitutions de n lettres, dont μ cycles sont A et dont tous les autres cycles sont B, est égal au nombre des substitutions de $n+1$ lettres, décomposables en $\mu+1$ cycles exactement, dont l'un, celui qui contient la lettre u_1, est un cycle β et dont tous les autres sont des cycles A.

Il serait facile de multiplier les théorèmes de ce genre; nous n'avons voulu en donner qu'un seul exemple. Sauf dans des cas particuliers, ils sont plus limpides, sous leur forme algébrique, que traduits en langage ordinaire.

Pour revenir aux polynômes $\bar{\omega}_n(x) = i^n H_n(-xi)$, examinés plus haut, nous en obtenons, par la formule (12), une troisième interprétation: le coefficient de x^μ, dans $\bar{\omega}_n(x)$, est égal au nombre des substitutions de $n+1$ lettres, décomposables en $\mu+1$ cycles exactement, dont l'un, celui qui contient une lettre déterminée u_1, est auto-conjugué d'ordre impair et dont les μ autres sont des cycles unités.

12. Donnons enfin la proposition suivante.

Soit R_n le nombre des substitutions de n lettres, dont un cycle, celui qui contient h lettres déterminées $u_1, u_2, \ldots u_h$, h étant fixe, indépendant de n, possède la propriété B et dont tous les autres cycles jouissent de la propriété A; on a

$$R_0 = R_1 = \cdots = R_{h-1} = 0, \quad R_h = b_h,$$

$$R_{n+1} = a_1 R_n + \binom{n-h}{1} a_2 R_{n-1} + \cdots + \binom{n-h}{h} a_{h+1} R_{n-h} + \cdots$$
$$+ b_{h+1} P_{n-h} + \binom{n-h}{1} b_{h+2} P_{n-h-1} + \cdots$$

et la fonction génératrice

$$\varrho(z) = R_h + R_{h+1} \frac{z}{1} + \cdots + R_n \frac{z^{n-h}}{(n-h)!} + \cdots$$

a pour valeur

$$\varrho(z) = e^{a(z)} \frac{d^h b(z)}{d z^h}.$$

On observera qu'ici la série $d^h b(z)/d z^h$ est majorée seulement par

$$\frac{(h-1)!}{(1-z)^h} = (h-1)! + h! \frac{z}{1} + (h+1)! \frac{z^2}{2} + \cdots,$$

ce qui donne une grande liberté d'interprétation de notre formule (6), dans les cas où l'interprétation donnée, lorsque les fonctions $a(z)$, $b(z)$, $c(z)$, sont majorées par $-\log(1-z)$, n'est plus applicable.

§ III.

Sur certaines familles de substitutions.

13. Nous ne ferons qu'énoncer rapidement quelques résultats relatifs au groupe alterné. On sait que, dans les substitutions de ce groupe, c'est-à-dire dans les substitutions paires, le nombre des cycles d'ordre pair est pair et que, dans les substitutions impaires, le nombre des cycles d'ordre pair est impair. Dès lors, la démonstration que nous avons donnée au § I, relativement à l'ensemble des substitutions de n lettres, c'est-à-dire relativement au groupe symétrique, se transpose sans difficulté aux familles de substitutions paires ou impaires, le fait que les substitutions paires forment un groupe n'intervenant en aucune façon, pas plus qu'il n'est intervenu dans le groupe symétrique.

Les nombres Q_n des substitutions paires et R_n des substitutions impaires, dont tous les cycles possèdent une propriété A, ont respectivement pour fonctions génératrices

$$(13)\qquad \begin{cases} \dfrac{e^{a(z)} + e^{-a(-z)}}{2} = \sum\limits_{n=0}^{\infty} Q_n \dfrac{z^n}{n!}, \\ \dfrac{e^{a(z)} - e^{-a(-z)}}{2} = \sum\limits_{n=0}^{\infty} R_n \dfrac{z^n}{n!}, \end{cases}$$

$$\begin{array}{ll} Q_0 = 1 & R_0 = 1 \\ Q_1 = a_1 & R_1 = 0 \\ Q_2 = a_1^2 & R_2 = a_2 \\ Q_3 = a_1^3 + a_3 & R_3 = 3\, a_1 a_2 \\ Q_4 = a_1^4 + 4\, a_1 a_3 + 3\, a_2^2 & R_4 = 6\, a_1^2 a_2 + a_4 \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots \end{array}$$

Le nombre $Q_n^{\lambda,\mu}$ des substitutions paires, dont λ cycles exactement sont A, dont μ cycles exactement sont B et dont tous les autres cycles sont C, a pour fonction génératrice

$$\frac{a^\lambda(z)}{\lambda!}\frac{b^\mu(z)}{\mu!}\frac{e^{c(z)}}{2} + (-1)^{\lambda+\mu}\frac{a^\lambda(-z)}{\lambda!}\frac{b^\mu(-z)}{\mu!}\frac{e^{-c(-z)}}{2} = \sum_{n=0}^{\infty} Q_n^{\lambda,\mu}\frac{z^n}{n!}.$$

Dans le polynôme $\xi_n(x, y)$, défini par

$$\frac{1}{2}\left[e^{a(z)+xb(z)+yc(z)} + e^{-a(-z)-xb(-z)-yc(-z)}\right] = \sum_{0}^{\infty} \xi_n(x, y)\frac{z^n}{n!}$$

le coefficient de $x^\lambda y^\mu$ est égal au nombre des substitutions du groupe alterné, de degré n, dont μ cycles sont C, dont λ cycles sont B et dont tous les cycles restants sont A.

Les autres résultats de nos paragraphes I et II s'étendraient de même; en particulier, il serait facile de former la suite des polynômes qui représentent les racines carrées de la substitution identique contenues dans le groupe alterné.

14. Pour généraliser les deux familles que constituent les substitutions paires et impaires, il semblerait naturel de répartir toutes les substitutions du groupe symétrique en k familles, suivant que le nombre des cycles, d'ordre multiple de k, est congru, (mod. k), à 0, à 1, à 2, ... ou à $k-1$. On obtient alors, en cherchant quel est dans chaque famille le nombre des substitutions, dont tous les cycles possèdent une propriété A, une certaine généralisation des équations (13). Mais les formules ainsi obtenues n'offrent pas la symétrie qu'on pourrait attendre et nous ne nous y arrêterons pas. Nous procéderons autrement.

En nous écartant de l'acception souvent admise[1] pour le mot »caractère», ce qui est sans inconvénient ici, nous appellerons caractère, (mod. m), d'une substitution une expression linéaire de la forme $an + b\nu$, prise suivant un certain module m, entier et fixe, n désignant le nombre des lettres et ν le nombre des cycles de cette substitution, et a et b deux nombres entiers. Chaque système de valeurs de a et b permet de répartir les substitutions en m familles, suivant que leur caractère

$$I_{ab} = an + b\nu$$

est congru, (mod. m), à 0, 1, 2, ... ou $m - 1$. Il y a donc m^2 systèmes possibles de m familles chacun. Il est clair que, suivant le module 2, les substitutions paires ont leur caractère $I_{1,1} = n + \nu$ congru à zéro, tandis que $I_{1,1}$ est congru à 1, pour les substitutions impaires.

Bornons-nous au cas où le module choisi est un nombre premier p. Le nombre p^2 des caractères possibles se réduit beaucoup, comme on va le voir.

En effet, le cas de $b = 0$ est sans intérêt, quel que soit a; il y a alors une famille, qui est le groupe symétrique tout entier et $p - 1$ familles nulles. Ensuite, si $a = 0$, il suffit de faire $b = 1$, car, p étant premier, les restes de 2ν, 3ν, 4ν, ..., (mod. p), sont les mêmes, à l'ordre près, que les restes de ν et, en donnant à b une valeur différente de 1, on ne fera que permuter entre elles les familles correspondant à $b = 1$. De même, il suffit de faire $a = 1$, $b = 1, 2, 3, \ldots, p - 1$, les autres valeurs $a = 2, 3, \ldots, p - 1$, ne faisant que permuter entre elles les familles qui correspondent aux cas où $a = 1$.

Restent donc seulement à considérer p systèmes de p familles chacun, ces systèmes étant définis par leurs caractères respectifs

$$I_{0,1} = \nu$$
$$I_{1,1} = n + \nu,\ I_{1,2} = n + 2\nu,\ \ldots\ I_{1,p-1} = n + (p - 1)\nu.$$

15. Supposons $p = 3$. Il y a alors trois caractères $I_{0,1}$, $I_{1,1}$, $I_{1,2}$. Relativement à chacun d'eux, $I_{\alpha\beta}$, nous désignerons par Q_n, R_n, S_n, le nombre des substitutions de n lettres, dont tous les cycles jouissent de la propriété A et pour lesquelles on a respectivement

$$I_{\alpha\beta} \equiv 0,\ I_{\alpha\beta} \equiv 1,\ I_{\alpha\beta} \equiv 2, \qquad \text{(mod. 3)}.$$

Les fonctions génératrices seront désignées par

[1] voir A. SPEISER — Die Theorie der Gruppen von endlicher Ordnung. — p. 118.

$$\chi(z) = \sum_0^\infty Q_n \frac{z^n}{n!},\ \varrho(z) = \sum_0^\infty R_n \frac{z^n}{n!},\ \sigma(z) = \sum_0^\infty S_n \frac{z^n}{n!},$$

et nous poserons de plus, j étant une racine cubique imaginaire de l'unité,

$$3\,Q_n = u_n + v_n + w_n$$
$$3\,R_n = u_n + j^2 v_n + j\,w_n$$
$$3\,S_n = u_n + j\,v_n + j^2 w_n$$

et, enfin,

$$U(z) = \sum_0^\infty u_n \frac{z^n}{n!},\ \ V(z) = \sum_0^\infty v_n \frac{z^n}{n!},\ \ W(z) = \sum_0^\infty w_n \frac{z^n}{n!}.$$

Les calculs étant similaires pour les trois caractères, développons-les seulement pour $I_{1,1} = n + \nu$ et calculons Q_{n+1}. Nous procéderons comme au § I, en engageant une $(n + 1)^{\text{ème}}$ lettre u_{n+1} dans un cycle d'ordre $p + 1$, ce qui se fera de $\binom{n}{p} a_{p+1}$ manières différentes, et en associant ce cycle, comme facteur, à une substitution partielle convenable de $n - p$ lettres. Je dis que:

$$Q_{n+1} = a_1 R_n + \binom{n}{1} a_2 Q_{n-1} + \binom{n}{2} a_3 S_{n-2} + \binom{n}{3} a_4 R_{n-3} + \cdots,$$

les lettres R, Q, S, se succédant périodiquement au second membre. En effet, soit ν' le nombre de cycles qui figurent dans une des substitutions qu'énumère Q_{n+1}, au premier membre; on doit avoir $n + 1 + \nu' \equiv 0$, (mod. 3), puisque ces substitutions permutent $n + 1$ lettres. D'autre part, dans chaque terme du second membre, le coefficient a_i symbolise un seul cycle. Si le facteur de a_i symbolise une substitution ayant ν cycles, on doit donc avoir $\nu = \nu' - 1$, puisque chaque substitution, symbolisée au second membre, l'est aussi au premier. Ainsi $\nu' = \nu + 1$ et l'on doit avoir, tout le long du second membre, pour les substitutions symbolisées par les majuscules R, S, T, la congruence $n + 1 + \nu + 1 \equiv 0$, (mod. 3), c'est-à-dire successivement $n + \nu \equiv 1$, $n - 1 + \nu \equiv 0$, $n - 2 + \nu \equiv 2$, $n - 3 + {}$ $+ \nu \equiv 1$, ..., (mod. 3); or, c'est bien ce qui a lieu dans notre formule récurrente, puisque, par la définition des familles Q, R, S, on a, pour les substitutions que symbolise $R_{n-\alpha}$, $n - \alpha + \nu \equiv 1$; pour celles que symbolise $S_{n-\beta}$, $n - \beta + \nu \equiv 2$, et pour celles que symbolise $Q_{n-\gamma}$, $n - \gamma + \nu \equiv 0$, (mod. 3). On trouverait, de même,

$$R_{n+1} = a_1 S_n + \binom{n}{1} a_2 R_{n-1} + \binom{n}{2} a_3 Q_{n-2} + \cdots$$

$$S_{n+1} = a_1 Q_n + \binom{n}{1} a_2 S_{n-1} + \binom{n}{2} a_3 R_{n-2} + \cdots$$

Les valeurs initiales à prendre sont $Q_0 = 1$, $R_0 = 0$, $S_0 = 0$, comme on s'en assure en formant le petit tableau d'indicateurs de cycles

$Q_0 = 1$	$R_0 = 0$	$S_0 = 0$
$Q_1 = 0$	$R_1 = 0$	$S_1 = a_1$
$Q_2 = a_2$	$R_2 = a_1^2$	$S_2 = 0$
$Q_3 = a_1^3$	$R_3 = a_3$	$S_3 = 3\, a_1 a_2$
$Q_4 = 4\, a_1 a_3 + 3\, a_2^2$	$R_4 = 6\, a_1^2 a_2$	$S_4 = a_1^4 + a_4$.

Des trois formules récurrentes pour Q_n, R_n, S_n, on tire les suivantes, pour u_n, v_n, w_n,

$$u_{n+1} = a_1 u_n + \binom{n}{1} a_2 u_{n-1} + \binom{n}{2} a_3 u_{n-2} + \cdots,$$

$$v_{n+1} = a_1 j^2 v_n + \binom{n}{1} a_2 v_{n-1} + \binom{n}{2} a_3 j\, v_{n-2} + \cdots,$$

$$w_{n+1} = a_1 j\, w_n + \binom{n}{1} a_2 w_{n-1} + \binom{n}{2} a_3 j^2 w_{n-2} + \cdots,$$

avec $u_0 = v_0 = w_0 = 1$ comme valeurs initiales, d'où, pour les fonctions $U(z)$, $V(z)$, $W(z)$, les expressions

$$U(z) = e^{a(z)}, \quad V(z) = e^{ja(jz)}, \quad W(z) = e^{j^2 a(j^2 z)}.$$

Finalement, les fonctions génératrices sont données par les formules

$$(14) \qquad \begin{cases} 3\,\chi(z) = e^{a(z)} + e^{ja(jz)} + e^{j^2 a(j^2 z)} \\ 3\,\varrho(z) = e^{a(z)} + j^2 e^{ja(jz)} + j\, e^{j^2 a(j^2 z)} \\ 3\,\sigma(z) = e^{a(z)} + j\, e^{ja(jz)} + j^2 e^{j^2 a(j^2 z)}, \end{cases}$$

qui sont bien une des généralisations que nous cherchions pour les deux formules (13).

Maintenant, pour le caractère $I_{1,2} = n + 2\nu$, on aura les formules de récurrence

$$Q_{n+1} = a_1 Q_n + \binom{n}{1} a_2 R_{n-1} + \binom{n}{2} a_3 S_{n-2} + \cdots,$$

$$R_{n+1} = a_1 R_n + \binom{n}{1} a_2 S_{n-1} + \binom{n}{2} a_3 Q_{n-2} + \cdots,$$

$$S_{n+1} = a_1 S_n + \binom{n}{1} a_2 Q_{n-1} + \binom{n}{2} a_3 R_{n-2} + \cdots,$$

$$Q_0 = 1, \qquad R_0 = 0, \qquad S_0 = 0,$$

et les triples des fonctions génératrices

$$(15) \qquad \begin{cases} 3\chi(z) = e^{a(z)} + e^{j^2 a(jz)} + e^{j a(j^2 z)} \\ 3\varrho(z) = e^{a(z)} + j e^{j^2 a(jz)} + j^2 e^{j a(j^2 z)} \\ 3\sigma(z) = e^{a(z)} + j^2 e^{j^2 a(jz)} + j e^{j a(j^2 z)}. \end{cases}$$

Enfin, pour le caractère $I_{0,1} = \nu$, on aura les triples des fonctions génératrices

$$\begin{cases} 3\chi(z) = e^{a(z)} + e^{j a(z)} + e^{j^2 a(z)} \\ 3\varrho(z) = e^{a(z)} + j^2 e^{j a(z)} + j e^{j^2 a(z)} \\ 3\sigma(z) = e^{a(z)} + j e^{j a(z)} + j^2 e^{j^2 a(z)} \end{cases}$$

qui ne dépendent que de la fonction $a(z)$ et ne constituent pas, à proprement parler, une généralisation des formules (13).

Malgré l'analogie des formules (14) ou (15) avec les formules (13), on sait qu'aucune des familles Q, R ou S ne peut constituer un groupe. Dans quelles conditions, le produit de deux substitutions d'une même famille passe-t-il dans une autre famille et dans laquelle, c'est ce qui exigerait une recherche que nous n'avons pas entreprise.

§ IV.

Sur les cycles secondaires.

16. Une substitution de n chiffres $1, 2, 3, \ldots n$, étant décomposée en cycles, soit C l'un d'eux. Nous supposerons toujours que, dans C, le chiffre le plus faible, parmi ceux que permute C, occupe la première place à gauche et nous appellerons cycle monotone C_M, correspondant à C, la substitution circulaire contenant les mêmes chiffres que C, mais rangés dans l'ordre croissant, à partir de la gauche. La substitution

$$\delta = \binom{C_M}{C},$$

où C_M et C sont deux permutations, C_M étant la permutation initiale et C la permutation finale, sera dite la décomposition secondaire du cycle primaire C. Les cycles de δ seront dits les cycles secondaires ou cycles de deuxième espèce de C. Le mot »cycle», quand il sera employé sans l'adjectif »secondaire», signifiera toujours cycle primaire ou cycle de première espèce. Si C, C', C'', ... sont les cycles primaires de S et C_M, C'_M, C''_M, ... les cycles monotones qui leur correspondent respectivement, la substitution $S_M = C_M C'_M C''_M \ldots$ sera dite la substitution à cycles monotones ou, plus simplement, la substitution monotone correspondant à S et la substitution $\varDelta = \delta\, \delta'\, \delta'' \ldots$, égale au produit des décompositions secondaires de C, C', C'', ... sera appelée la décomposition secondaire de S.

17. La substitution S étant donnée, S_M et $\varDelta$ sont déterminées. S_M est une substitution semblable à S et, inversement, quand S_M et $\varDelta$ sont données, S est déterminée. Il est visible, en effet, que S s'obtient en effectuant, dans les cycles de S_M, la substitution $\varDelta = \delta\, \delta'\, \delta'' \ldots$; autrement dit, S est la transformée de S_M par $\varDelta$,

$$S = \varDelta^{-1} S_M \varDelta,$$

les opérations étant effectuées dans l'ordre où elles sont écrites, c'est-à-dire en commençant par $\varDelta^{-1}$ et en finissant par $\varDelta$. Lorsque S et S_M sont données, $\varDelta$ n'est donc déterminée qu'à un facteur U près, qui est permutable à S_M et alors U est facteur à gauche, c'est-à-dire s'écrit à gauche de $\varDelta$, ou qu'à un facteur V près, qui est permutable à S et alors V est facteur à droite de $\varDelta$.

Pour connaître la substitution monotone S_M, qui correspond à une substitution S, il suffit de connaître les chiffres qui figurent dans chaque cycle de S; il n'est pas nécessaire de connaître l'ordre de succession de ces chiffres dans le cycle qui les renferme. Inversement, une substitution monotone S_M étant donnée et étant décomposable en k cycles, d'ordres $\alpha_1, \alpha_2, \ldots \alpha_k$, égaux ou inégaux, il y a $\Gamma(\alpha_1)\,\Gamma(\alpha_2) \ldots \Gamma(\alpha_k)$ substitutions S, qui admettent S_M comme substitution monotone et la somme $\Sigma\, \Gamma(\alpha_1)\,\Gamma(\alpha_2) \ldots \Gamma(\alpha_k)$, étendue à toutes les substitutions monotones de n chiffres, est égale à $\Gamma(n+1) = n!$.

Les cycles primaires des substitutions monotones sont représentés géométriquement par des polygônes convexes, décrits dans un sens déterminé. D'après la formule (4) du § I, le nombre μ_n des substitutions monotones de n chiffres, ayant k_i cycles primaires d'ordre i, $(i = 1, 2, 3, \ldots n)$, est donc

$$\mu_n = \frac{1}{k_1!\, k_2! \ldots k_n!} \frac{n!}{(1!)^{k_1} (2!)^{k_2} \ldots (n!)^{k_n}},$$

$$k_1 + 2k_2 + \cdots + ik_i + \cdots + nk_n = n.$$

Quant aux cycles secondaires d'une substitution monotone, ce sont tous des cycles unités.

Toute décomposition secondaire $\varDelta$ comporte au moins un cycle unité, contenant le chiffre le plus faible, le cycle (1) et, réciproquement, pour qu'une décomposition secondaire, donnée à l'avance, soit admissible, il suffit qu'elle contienne le cycle unité (1). En effet, il existe toujours alors une et une seule substitution circulaire S, de n chiffres, qui admet la décomposition secondaire $\varDelta$. S est la transformée par $\varDelta$ du cycle monotone $(1, 2, 3, \ldots n)$. Il y a donc $(n-1)!$ décompositions secondaires distinctes des substitutions de n chiffres; on les obtient en multipliant par le cycle unité (1) toutes les décompositions en cycles primaires des substitutions des $n-1$ chiffres $2, 3, \ldots n-1, n$.

Tout cycle primaire, d'ordre > 1, d'une substitution S donne naissance à au moins deux cycles secondaires. L'ordre maximum des cycles de $\varDelta$, décomposition secondaire de S, est donc inférieur d'une unité, au moins, à l'ordre maximum des cycles de S, le cas où S serait la substitution identique étant seul excepté. Supposons que S contienne α cycles primaires d'ordre 1 et β cycles primaires d'ordre > 1, le nombre des cycles de $\varDelta$ sera $\geq \alpha + 2\beta$. De là résulte que, si le nombre des chiffres permutés est supérieur à deux et si la décomposition secondaire $\varDelta$ n'est formée que de deux cycles, $\varDelta$ ne peut appartenir qu'à une substitution circulaire des n chiffres. Faisons, en effet, $\alpha + 2\beta = 2$. Si $\alpha = 2$, $\beta = 0$; il n'y a alors que deux chiffres permutés, ce qui est exclus. Si $\alpha = 0$, $\beta = 1$; alors S n'a qu'un seul cycle et est déterminée, comme nous l'avons vu, d'une manière unique, par sa décomposition secondaire $\varDelta$.

Pour qu'une décomposition secondaire $\varDelta$ détermine, d'une manière unique, la substitution S qui l'admet, il faut et il suffit que $\varDelta$ ne contienne qu'un seul cycle d'ordre 1, savoir le cycle (1). Alors S est circulaire et $\varDelta$ est le produit du cycle (1) par une substitution d'Euler, sans rencontres, des $n-1$ chiffres $2, 3, \ldots .\, n-1,\ n$. En effet, la substitution S, si elle est circulaire, est déterminée d'une manière unique par $\varDelta$; si elle n'est pas circulaire, elle a au moins deux cycles et alors $\varDelta$ a au moins deux cycles unités. Inversement, si $\varDelta$ a deux cycles unités, (1) et (α), on peut former d'abord une substitution circulaire qui admet $\varDelta$ et ensuite une substitution, composée de deux cycles primaires, par exemple la substitution $(1, \beta, \gamma, \delta, \ldots)(\alpha)$, qui admet aussi la décomposition secondaire Δ.

Plus généralement, si une décomposition secondaire Δ contient p cycles d'ordre 1, les substitutions S, qui admettent Δ, ont 1 ou 2 ou 3 .... ou p cycles primaires et on peut toujours former au moins p substitutions qui admettent la décomposition secondaire Δ. En effet, en prenant $p = 3$, par exemple, supposons que $\Delta = (1)(\alpha)(\beta)\Delta'$; on formera d'abord une substitution circulaire admettant Δ; puis, une substitution formée du produit de (α) par une substitution circulaire admettant $(1)(\beta)\Delta'$, comme décomposition secondaire; puis une substitution, formée du produit de $(\alpha)(\beta)$ par une substitution circulaire admettant $(1)\Delta'$, comme décomposition secondaire.

18. Je me propose maintenant de chercher, d'une façon précise, quel est le nombre des substitutions qui admettent une décomposition secondaire donnée Δ. Soient

$$(1), (\alpha_1), (\alpha_2), \ldots (\alpha_i), \ldots (\alpha_{\mu-1}),$$

les cycles unités de Δ, où

$$1 < \alpha_1 < \alpha_2 < \cdots < \alpha_i < \cdots < \alpha_{\mu-1}.$$

Nous désignerons par $A_1^i, A_2^i, \ldots A_{m_i}^i$ les cycles de Δ, au nombre de m_i, qui ne contiennent que des chiffres supérieurs à α_i, en comprenant, dans ce nombre m_i, les cycles $(\alpha_{i+1}), (\alpha_{i+2}), \ldots (\alpha_{\mu-1})$. Alors, si $\alpha_i < \alpha_j$, on a évidemment $m_i > m_j$ et $i < j$.

Cela posé, nous allons chercher à former, non pas les cycles primaires eux-mêmes des substitutions qui admettent la décomposition secondaire Δ, mais les diverses manières de constituer la décomposition secondaire partielle de chacun de ces cycles primaires et nous compterons ces diverses manières. Cette façon de procéder est suffisante, puisqu'il y aura une substitution circulaire unique, c'est-à-dire un seul cycle qui admettra une décomposition secondaire partielle, une fois que celle-ci aura été formée.

Les substitutions qui admettent Δ sont:

Premièrement. — Une seule substitution circulaire S_1.

Deuxièmement. — Des substitutions S_2, formées de deux cycles primaires. Le premier de ces cycles commence par le chiffre 1; le deuxième par le chiffre α_1 ou α_2 .... ou $\alpha_{\mu-1}$. S'il commence par α_i, il faut, dans la décomposition secondaire partielle δ qui lui correspond, associer le cycle (α_i) à des cycles de Δ, ne contenant que des chiffres supérieurs à α_i, c'est-à-dire à des cycles choisis dans la suite $A_1^i, A_2^i, \ldots A_{m_i}^i$. Le cycle secondaire (1) sera alors associé lui-même à tous les cycles de $\varDelta$, qui n'auront pas été associés au cycle (α_i). Or, on peut associer (α_i) soit à un seul des cycles A_e^i, soit à une combinaison deux à deux, $A_e^i A_g^i$, soit à une combinaison trois à trois, $A_e^i A_g^i A_h^i$, etc. Il y a donc, i étant fixé,

$$1 + \binom{m_i}{1} + \binom{m_i}{2} + \cdots + \binom{m_i}{m_i} = 2^{m_i}$$

décompositions partielles du cycle commençant par le chiffre α_i et, en sommant, pour $i = 1, 2, 3, \ldots \mu - 1$, nous voyons que le nombre des substitutions S_2 est égal à

$$2^{m_1} + 2^{m_2} + \cdots + 2^{m_{\mu-1}} = \frac{1}{1!} \sum 2^{m_i}.$$

Troisièmement. — Des substitutions S_3, formées de trois cycles primaires. L'un d'eux commence par le chiffre 1, le second par le chiffre α_i, le troisième par le chiffre α_j, où $i < j$. On peut, comme troisième cycle, prendre (α_j) seul et on est ramené au »Deuxièmement», c'est-à-dire à trouver les substitutions composées de deux cycles, qui admettent une décomposition secondaire $\varDelta'$, pour laquelle les nombres m_ϱ sont remplacés par $m_\varrho - 1$, puisqu'il y a un cycle en moins, savoir le cycle (α_j). Nous obtenons ainsi $\frac{1}{1!} \sum\limits_i 2^{m_i - 1}$ formes de $\varDelta'$. On peut prendre ensuite, comme décomposition secondaire du troisième cycle, (α_j) associé à une combinaison un à un des cycles $A_1^j, \ldots A_{m_j}^j$. On est ramené au »Deuxièmement», c'est-à-dire à dénombrer des substitutions, formées de deux cycles, qui admettent une décomposition secondaire $\varDelta'$, pour laquelle les nombres m_ϱ sont remplacés par $m_\varrho - 2$, puisqu'il y a deux cycles en moins, le cycle (α_j) et l'un des cycles A_e^j. On obtient ainsi

$$\binom{m_j}{1} \frac{1}{1!} \sum_i 2^{m_i - 2}.$$

On peut ensuite associer (α_j) à une combinaison deux à deux des cycles A_1^j, $A_2^j, \ldots A_{m_j}^j$ et on est ramené au »Deuxièmement», où les nombres m_ϱ sont remplacés par $m_\varrho - 3$, d'où le terme

$$\binom{m_j}{2} \frac{1}{1!} \sum_i 2^{m_i - 3},$$

et ainsi de suite.

En ajoutant ces divers termes, on a

$$\frac{1}{1!}\sum_i 2^{m_i-1}\left[1+\binom{m_j}{1}\frac{1}{2}+\binom{m_j}{2}\frac{1}{2^2}+\cdots\right]=\frac{1}{1!}\sum_i 2^{m_i-1}\left(\frac{3}{2}\right)^{m_j},$$

et il faut maintenant sommer pour $j = 2, 3, \ldots \mu - 1$, ce qui nous donne, pour le nombre des substitutions S_3, l'expression

$$\frac{1}{1!}\sum_{i,j} 2^{m_i-1}\left(\frac{3}{2}\right)^{m_j}, \quad i<j,$$

que l'on peut écrire

$$\frac{1}{2!}\sum_{i,j}\left(\frac{2}{1}\right)^{m_i}\left(\frac{3}{2}\right)^{m_j}, \quad i<j.$$

Quatrièmement. — Des substitutions S_4, formées de quatre cycles primaires. En suivant une marche similaire, c'est-à-dire en étudiant le mode de formation du quatrième cycle, commençant par le chiffre α_k, on est ramené à sommer des expressions qui sont connues, d'après le »Troisièmement» et on trouve que le nombre des substitutions S_4 est égal à

$$\frac{1}{3!}\sum_{i,j,k}\left(\frac{2}{1}\right)^{m_i}\left(\frac{3}{2}\right)^{m_j}\left(\frac{4}{3}\right)^{m_k}, \quad i<j<k.$$

Supposons démontré que le nombre des substitutions S_p, admettant $\varDelta$ et composées de p cycles, soit

$$\frac{1}{(p-1)!}\sum_{i,j\ldots r}\left(\frac{2}{1}\right)^{m_i}\left(\frac{3}{2}\right)^{m_j}\cdots\left(\frac{p}{p-1}\right)^{m_r}, \quad i<j<\cdots<r,$$

Alors,

$(p+1)$-èmement. — Les substitutions qui admettent $\varDelta$ comprennent des substitutions S_{p+1}, formées de $p+1$ cycles primaires. L'un commence par le chiffre 1, le deuxième par α_i, le troisième par α_j, ... le $(p+1)$-ème par α_s, $1<\alpha_i<\alpha_j<\cdots<\alpha_s$, d'où $1<i<j<\cdots<s$. Pour former la décomposition secondaire de ce $(p+1)$-ème cycle, on prend le cycle (α_s) seul et on est ramené au »p-èmement» où les nombres m_ϱ sont remplacés par $m_\varrho - 1$, d'où le terme

$$\frac{1}{(p-1)!}\sum_{i,j,\ldots,r}\left(\frac{2}{1}\right)^{m_i-1}\cdots\left(\frac{p}{p-1}\right)^{m_r-1};$$

on prend ensuite (α_s) associé à une combinaison un à un des cycles $A_1^s, \ldots A_{m_s}^s$

et on est ramené au »p-èmement», où les nombres m_ϱ sont remplacés par $m_\varrho - 2$, d'où le terme

$$\binom{m_s}{1} \frac{1}{(p-1)!} \sum_{i,j,\ldots r} \left(\frac{2}{1}\right)^{m_i-2} \cdots \left(\frac{p}{p-1}\right)^{m_r-2},$$

et ainsi de suite.

Ajoutons ces expressions et il vient

$$\frac{1}{(p-1)!} \sum_{i,j,\ldots r} \left(\frac{2}{1}\right)^{m_i-1} \left(\frac{3}{2}\right)^{m_j-1} \cdots \left(\frac{p}{p-1}\right)^{m_r-1} \Bigg[1 + \\ + \binom{m_s}{1} \left(\frac{1}{2}\frac{2}{3} \cdots \frac{p-1}{p}\right)^{-1} + \binom{m_s}{2} \left(\frac{1}{2}\frac{2}{3} \cdots \frac{p-1}{p}\right)^{-2} + \cdots \Bigg] = \\ = \frac{1}{(p-1)!} \sum_{i,j,\ldots r} \left(\frac{2}{1}\right)^{m_i-1} \cdots \left(\frac{p}{p-1}\right)^{m_r-1} \left(\frac{p+1}{p}\right)^{m_s}.$$

Il reste à sommer par rapport à s et l'on voit que le nombre des substitutions S_{p+1} peut s'écrire

$$\frac{1}{p!} \sum_{i,j,\ldots s} \left(\frac{2}{1}\right)^{m_i} \left(\frac{3}{2}\right)^{m_j} \cdots \left(\frac{p+1}{p}\right)^{m_s}.$$

La formule, supposée démontrée pour p, l'est donc pour $p+1$; or elle l'est pour $p = 1, 2, 3$ et 4.

En résumé, en reprenant les notations indiquées au début de ce numéro, les substitutions S, admettant une décomposition secondaire donnée $\varDelta$, contenant μ cycles unités, comprennent

1°) Une substitution circulaire S_1 et une seule.

2°) Des substitutions S_2, formées de deux cycles primaires; leur nombre est

$$\frac{1}{1!} \sum 2^{m_i}.$$

3°) Des substitutions S_3 formées de trois cycles primaires; leur nombre est

$$\frac{1}{2!} \sum \left(\frac{2}{1}\right)^{m_i} \left(\frac{3}{2}\right)^{m_j}, \quad i < j$$

4°) Des substitutions S_4 formées de quatre cycles primaires; leur nombre est

$$\frac{1}{3!} \sum \left(\frac{2}{1}\right)^{m_i} \left(\frac{3}{2}\right)^{m_j} \left(\frac{4}{3}\right)^{m_k}, \quad i < j < k$$

. . . .

μ°) Des substitutions S_μ, formées de μ cycles primaires; leur nombre est

$$\frac{1}{(\mu-1)!}\left(\frac{2}{1}\right)^{m_1}\left(\frac{3}{2}\right)^{m_2}\left(\frac{4}{3}\right)^{m_3}\cdots\left(\frac{\mu}{\mu-1}\right)^{m_{\mu-1}}.$$

19. Observons qu'on a toujours

$$m_1 \geq \mu - 2,\ m_2 \geq \mu - 3,\ \ldots\ m_{\mu-1} \geq 0;$$

en particulier, si le nombre μ des cycles unités de la substitution $\varDelta$ est égal au nombre n des chiffres permutés, tous les cycles secondaires des substitutions admettant $\varDelta$ comme décomposition secondaire, seront d'ordre 1. Ces substitutions seront donc toutes les substitutions monotones de n chiffres et on obtiendra leur nombre en additionnant les expressions du numéro précédent, après y avoir fait $m_1 = n-2, \ldots\ m_i = n-i-1, \ldots$ Nous avons déjà obtenu ce nombre au numéro 3 du § I, sous une autre forme et on peut encore en obtenir d'autres expressions par des moyens différents.

Dans le cas général, on peut donner une formule symbolique, qui représente le nombre N des substitutions admettant une décomposition secondaire $\varDelta$, en procédant de la manière suivante. Considérons le développement en série entière de

$$1 + \frac{x}{1-x} + \frac{y}{1-y}\,\frac{xy}{1-xy} + \frac{z}{1-z}\,\frac{yz}{1-yz}\,\frac{xyz}{1-xyz} + \cdots.$$

La première fraction donne des termes en x^α, la deuxième des termes en $x^\alpha y^{\alpha+\beta}$, la troisième des termes en $x^\alpha y^{\alpha+\beta} z^{\alpha+\beta+\gamma}, \ldots\ \alpha = 1, 2, \ldots, \beta = 1, 2, \ldots, \gamma = 1, 2, \ldots$. Si donc nous posons

$$a_i = \frac{1}{1}\left(\frac{2}{1}\right)^{m_i}, \text{ pour } i = 1, 2, \ldots\ \mu-1,$$

$$a_i = 0, \qquad \text{pour } i \geq \mu,$$

$$b_i = \frac{1}{2}\left(\frac{3}{2}\right)^{m_i}, \text{ pour } i = 1, 2, \ldots\ \mu-1,$$

$$b_i = 0, \qquad \text{pour } i \geq \mu,$$

$$c_i = \frac{1}{3}\left(\frac{4}{3}\right)^{m_i}, \text{ pour } i = 1, 2, \ldots\ \mu-1,$$

$$c_i = 0, \qquad \text{pour } i \geq \mu,$$

etc., μ étant le nombre des cycles unités de $\varDelta$, nous aurons symboliquement, c'est-à-dire en remplaçant les exposants de $a, b, c, \ldots$ par des indices,

$$N = 1 + \frac{a}{1-a} + \frac{b}{1-b}\,\frac{ab}{1-ab} + \frac{c}{1-c}\,\frac{bc}{1-bc}\,\frac{abc}{1-abc} + \cdots.$$

20. Il est naturel de se demander si on peut former des groupes avec les substitutions à cycles monotones. La réponse est facile à donner. L'inverse du cycle monotone $(1, 2, 3, \ldots k-1, k)$ est $(1, k, k-1, \ldots 3, 2)$; il n'est donc monotone que si $k=2$. Pour former un groupe, des substitutions monotones doivent donc être d'ordre 2. Soient alors S et T deux substitutions d'ordre 2; leur produit doit être d'ordre 2 aussi; on a donc $S^2 = 1$, $T^2 = 1$, $STST = 1$, d'où l'on déduit $ST = TS$. Les seuls groupes que l'on puisse former avec des substitutions monotones sont donc tous les groupes abéliens, dont les éléments sont des racines carrées de la substitution identique. Ces groupes, qui se présentent dans la théorie des substitutions linéaires, sont connus depuis longtemps.

§ V.

Propriétés des cycles secondaires.

21. Je me propose de trouver la fonction génératrice du nombre Q_n ou $Q_n(a)$ des substitutions de n lettres, dont tous les cycles secondaires possèdent une certaine propriété A. Je continuerai à appeler $a(z)$ la fonction génératrice des nombres $a_1, a_2, a_3, \ldots$ de substitutions circulaires qui jouissent de cette propriété et je désignerai, dans tout ce paragraphe, par P_n ou $P_n(a)$ ou, éventuellement, $P_n(a_1, a_2, \ldots a_n)$ les polynômes indicateurs de cycles primaires, définis, au § I, par la formule (2) et dont j'ai donné le tableau (3).

Remarquons tout de suite qu'une décomposition secondaire contenant toujours au moins un cycle unité, il est nécessaire que $a_1 = 1$, c'est-à-dire que la propriété A doit nécessairement appartenir aux cycles d'une lettre. Cela étant, supposons connus $Q_1, Q_2, \ldots Q_n$ et aux n lettres $u_1, u_2, \ldots u_n$, adjoignons une $(n+1)$-ème lettre u_{n+1}, pour calculer Q_{n+1}.

La lettre u_{n+1} peut entrer dans un cycle primaire d'ordre $1, 2, 3, \ldots$ ou $n+1$; supposons qu'elle entre dans un cycle C, d'ordre $p+1$; elle sera associée à l'une des $\binom{n}{p}$ combinaisons p à p des n premières lettres. Soit alors Γ le cycle monotone, correspondant à C; la substitution, par laquelle on passe de la permutation Γ à la permutation C, définit, par ses cycles primaires, les cycles secondaires de C. Cette substitution se décompose en un cycle unité, qui jouit de la propriété A, et en une substitution de p lettres, dont tous les cycles

35—38333. *Acta mathematica*. 70. Imprimé le 7 février 1939.

primaires doivent posséder la propriété A. Le nombre de ces substitutions est $P_p(a)$. De plus, le cycle C devra être associé, comme facteur, à l'une des $Q_{n-p}(a)$ substitutions des $n-p$ lettres restantes, dont tous les cycles secondaires possèdent la propriété A, d'où la formule de récurrence

$$(16)\qquad Q_{n+1} = a_1 P_0 Q_n + \binom{n}{1} a_1 P_1 Q_{n-1} + \cdots + \binom{n}{p} a_1 P_p Q_{n-p} + \cdots.$$

Le dernier terme à droite est $a_1 P_n Q_0$; il est relatif à des substitutions circulaires de $n+1$ lettres; on doit donc faire $Q_0 = 1$. Soit

$$(17)\qquad Q(z) = \sum_{n=0}^{\infty} Q_n \frac{z^n}{n!};$$

on tire de (16)

$$Q'(z) = a_1 e^{a(z)} Q(z)$$

et, en intégrant,

$$(18)\qquad Q(z) = e^{a_1 \int_0^z e^{a(z)} dz}.$$

L'équation récurrente (16) nous donne, de proche en proche, les indicateurs de cycles secondaires:

$$(19)\quad \begin{cases} Q_0 = 1 \\ Q_1 = a_1 \\ Q_2 = 2\,a_1^2 \\ Q_3 = 5\,a_1^3 + a_1 a_2 \\ Q_4 = 15\,a_1^4 + 7\,a_1^2 a_2 + a_1 a_3 \\ Q_5 = 52\,a_1^5 + 41\,a_1^3 a_2 + 9\,a_1^2 a_3 + 3\,a_1 a_2^2 + a_1 a_4 \\ Q_6 = 203\,a_1^6 + 236\,a_1^4 a_2 + 64\,a_1^3 a_3 + 43\,a_1^2 a_2^2 + 11\,a_1^2 a_4 + 10\,a_1 a_2 a_3 + a_1 a_5 \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Le coefficient de a_1^n, dans Q_n, est égal au nombre ω_n des substitutions monotones de n lettres, puisque tous les cycles secondaires de ces substitutions sont des cycles unités.

Le tableau (19) est relatif aux substitutions dont tous les cycles possèdent la propriété A. Pour avoir les indicateurs de cycles relatifs à tout le groupe symétrique on fera comme précédemment $a_\nu = (\nu - 1)!\, x_\nu$, $(\nu = 1, 2, 3, \ldots)$ et l'on aura sous les yeux la constitution de toutes les substitutions de ce groupe, au moyen de leurs cycles secondaires. Maintenant, en comparant la formule (16) à la formule (1) du § I, on voit que si, dans cette dernière, on remplace a_1 par $a_1 P_0$, a_2 par $a_1 P_1$, ... a_i par $a_1 P_{i-1}$, ... on obtient (16). L'équation (4) nous donne donc l'expression générale

$$Q_n = \sum \frac{n!}{\alpha_1! \, \alpha_2! \ldots \alpha_n!} \left(\frac{a_1 P_0}{1}\right)^{\alpha_1} \left(\frac{a_1 P_1}{2!}\right)^{\alpha_2} \cdots \left(\frac{a_1 P_{n-1}}{n!}\right)^{\alpha_n}, \tag{20}$$

où $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$, mais cette expression n'est pas explicite en a_1, a_2, ... a_{n-1}, et il semble assez difficile d'obtenir une telle formule explicite. Appliquons-la cependant au cas où tous les nombres a_ν sont égaux à l'unité; Q_n sera le nombre des substitutions de n lettres, dont tous les cycles secondaires sont représentés géométriquement par des polygônes convexes, décrits dans un sens déterminé. On aura, d'après (18),

$$Q(z) = e^{\int_0^z e^{e^z - 1} dz},$$

qui s'exprime au moyen du logarithme intégral et l'on devra, dans (20), remplacer $a_1 P_i$ par ω_i, nombre des substitutions monotones de i lettres.

22. Cherchons maintenant le nombre Q_n^λ ou $Q_n^\lambda(a, \lambda b)$ des substitutions de n lettres, dont λ cycles secondaires exactement sont B et dont tous les autres cycles secondaires sont A. Il y a ici deux cas à distinguer, suivant que c'est la propriété A ou la propriété B qui appartient aux cycles d'une lettre. Le raisonnement à employer diffère peu de celui du numéro 21 et se lit d'ailleurs clairement sur les formules récurrentes que nous allons écrire. Nous désignerons par P_n^k ou $P_n^k(a, k b)$ le nombre des substitutions de n lettres, dont k cycles primaires exactement sont des cycles B et dont tous les autres cycles primaires sont des cycles A.

23. Dans le premier cas, où la propriété A appartient aux cycles d'une lettre, $a_1 = 1$ et, par suite, $b_1 = 0$, puisque les propriétés A et B s'excluent. On a alors

$$Q_{n+1}^\lambda = a_1 Q_n^\lambda + \binom{n}{1}\left[a_1 P_1(a)\, Q_{n-1}^\lambda + a_1 P_1^1(a, b) Q_{n-1}^{\lambda-1}\right] + \cdots \tag{21}$$

$$+ \binom{n}{p}\left[a_1 P_p(a)\, Q_{n-p}^\lambda + a_1 P_p^1(a, b)\, Q_{n-p}^{\lambda-1} + \cdots + a_1 P_p^\lambda(a, \lambda b)\, Q_{n-p}^0\right] + \cdots + a_1 P_n^\lambda(a, \lambda b).$$

Les valeurs initiales sont

$$Q_p^\lambda = 0, \text{ si } p < \lambda; \; Q_\lambda^\lambda = 0, \text{ sauf } Q_0^0 = 1;$$

$$P_p^\lambda = 0, \text{ si } p < \lambda; \; P_\lambda^\lambda = 0, \text{ sauf } P_0^0 = 1.$$

Soit

$$Q_\lambda(z) = \sum_{n=0}^{\infty} Q_n^\lambda \frac{z^n}{n!};$$

la relation (21) nous donne l'équation différentielle

$$(22) \qquad \frac{d}{dz} Q_\lambda(z) = a_1 e^{a(z)} Q_\lambda(z) + a_1 \frac{b(z)}{1} e^{a(z)} Q_{\lambda-1}(z) + a_1 \frac{b^2(z)}{2!} e^{a(z)} Q_{\lambda-2}(z) + \cdots + a_1 \frac{b^\lambda(z)}{\lambda!} e^{a(z)} Q_0(z),$$

que l'on peut intégrer de proche en proche, avec l'aide des conditions initiales et en remarquant que $Q_0(z)$ n'est autre que la fonction (18). Mais on peut opérer plus rapidement; soit

$$(23) \qquad U(z) = Q_0(z) + y\, Q_1(z) + y^2 Q_2(z) + \cdots.$$

D'après (22), on a

$$\frac{dU}{dz} = a_1 e^{a(z)} e^{y\,b(z)} U(z),$$

d'où en intégrant,

$$U(z) = e^{a_1 \int_0^z e^{a(z)+y\,b(z)} dz}$$

Posons

$$(24) \qquad A(z) = \int_0^z e^{a(z)} dz \quad \text{et} \quad B_\nu(z) = \int_0^z [b(z)]^\nu e^{a(z)} dz, \qquad (\nu = 0, 1, 2, \ldots),$$

il vient

$$U(z) = e^{a_1 A(z)} e^{a_1 B_1(z) \frac{y}{1} + a_1 B_2(z) \frac{y^2}{2!} + \cdots}$$

et, en nous rappelant que

$$e^{x_1 \frac{y}{1} + x_2 \frac{y^2}{2!} + x_3 \frac{y^3}{3!} + \cdots} = \sum_{\nu=0}^{\infty} \frac{y^\nu}{\nu!} P_\nu(x_1, x_2, \ldots x_\nu).$$

l'identification des termes en y, dans (23) et dans le développement de l'exponentielle $U(z)$, nous donne l'expression cherchée de $Q_\lambda(z)$,

$$Q_\lambda(z) = \frac{1}{\lambda!} e^{a_1 A(z)} P_\lambda(a_1 B_1, a_1 B_2, \dots a_1 B_\lambda).$$

24. Dans le deuxième cas, où c'est la propriété B qui appartient aux cycles d'une lettre, $b_1 = 0$ et $a_1 = 1$. Pour éviter une confusion, remplaçons la lettre Q par la lettre χ et nous aurons

$$\chi_{n+1}^\lambda = b_1 \chi_n^{\lambda-1} + \binom{n}{1}[b_1 P_1(a)\chi_{n-1}^{\lambda-1} + b_1 P_1^1(a,b)\chi_{n-1}^{\lambda-2}] + \cdots$$
$$+ \binom{n}{p}[b_1 P_p(a)\chi_{n-p}^{\lambda-1} + b_1 P_p^1(a,b)\chi_{n-p}^{\lambda-2} + \cdots + b_1 P_p^{\lambda-1}(a,(\lambda-1)b)\chi_{n-p}^0] + \cdots$$

avec les conditions initiales

$$\chi_p^\lambda = 0, \text{ si } p < \lambda; \ \chi_0^0 = 1, \ \chi_\lambda^\lambda = \omega_\lambda;$$
$$P_p^\lambda = 0, \text{ si } p < \lambda; \ P_0^0 = 1, \ P_\lambda^\lambda = 1;$$

où ω_λ a la même signification qu'au numéro 21. Pour la fonction génératrice

$$\chi_\lambda(z) = \sum_{n=0}^{\infty} \chi_n^\lambda \frac{z^n}{n!},$$

on aura la relation

$$\chi_\lambda'(z) = b_1 e^{a(z)}\chi_{\lambda-1}(z) + b_1 \frac{b(z)}{1} e^{a(z)}\chi_{\lambda-2}(z) + b_1 \frac{b^2(z)}{2!} e^{a(z)}\chi_{\lambda-3}(z) + \cdots$$

avec $\chi_0(z) = 1$.

On en tire, pour la fonction $V(z) = \chi_0(z) + y\chi_1(z) + \cdots + y^\nu \chi_\nu(z) + \cdots$ l'équation

$$\frac{d}{dz}\frac{V(z) - \chi_0(z)}{y} = \frac{1}{y}\frac{d\,V(z)}{dz} = b_1 V(z) e^{a(z) + y b(z)},$$

d'où, en intégrant,

$$\log V(z) = b_1 \int_0^z y e^{a(z) + y b(z)} dz$$

et, en procédant comme tout à l'heure, on trouve enfin

$$\chi_\lambda(z) = \frac{1}{\lambda!} P_\lambda(b_1 B_0, \ 2 b_1 B_1, \ 3 b_1 B_2, \dots \lambda b_1 B_{\lambda-1}).$$

25. Indiquons rapidement les résultats suivants.

Les nombres g_n des substitutions paires de n lettres et h_n des substitutions impaires, dont tous les cycles secondaires possèdent une propriété A, ont respectivement pour fonctions génératrices

$$\frac{e^{A(z)} + e^{-A(-z)}}{2} = \sum_0^\infty g_n \frac{z^n}{n!}, \quad \frac{e^{A(z)} - e^{-A(-z)}}{2} = \sum_0^\infty h_n \frac{z^n}{n!},$$

$A(z)$ étant définie par l'équation (24).

Répartissons les substitutions du groupe symétrique en deux familles, les substitutions de la première famille ayant un nombre pair de cycles secondaires d'ordre pair, les substitutions de la deuxième famille ayant un nombre impair de cycles secondaires d'ordre pair; le nombre G_n des substitutions de la première famille et le nombre H_n des substitutions de la deuxième famille, dont tous les cycles secondaires possèdent la propriété A, ont respectivement pour fonctions génératrices

$$\frac{e^{A(z)} + e^{\alpha(z)}}{2} = \sum_{n=0}^\infty G_n \frac{z^n}{n!}, \quad \frac{e^{A(z)} - e^{\alpha(z)}}{2} = \sum_{n=0}^\infty H_n \frac{z^n}{n!},$$

où $A(z)$ a la signification (24) et où

$$\alpha(z) = \int_0^z e^{-a(-z)}\, dz.$$

En particulier, si la propriété A convient à tous les cycles, quels qu'ils soient, on a

$$2\, G_n = n! + \bar{\omega}_n(1), \quad 2\, H_n = n! - \bar{\omega}_n(1),$$

$\bar{\omega}_n(x)$ étant le polynôme, lié aux polynômes d'Hermite, que nous avons introduit au § II.

25. J'envisage maintenant deux questions où interviennent à la fois des cycles primaires et des cycles secondaires.

Cherchons d'abord le nombre $R_n(\lambda a, b)$ des substitutions de n lettres, dont λ cycles primaires exactement, C', C'', ... $C^{(\lambda)}$, ont la propriété A et dont tous les cycles secondaires, dérivés des cycles primaires, autres que C', C'', ... $C^{(\lambda)}$, ont la propriété B.

Quelques remarques préalables sont nécessaires. Si nous formons un cycle primaire Γ, tel que tous ses cycles secondaires possèdent la propriété B, il faut, pour pouvoir conduire le calcul, que nous soyons certains que Γ, en tant que cycle primaire, ne possède pas la propriété A. Autrement dit, les deux hypothèses, »Γ, cycle primaire, possède la propriété A» et »Tous les cycles secondaires de Γ, sans exception, possèdent la propriété B», s'excluent mutuellement. Soit alors une certaine combinaison de $p+1$ lettres; nous pouvons former $p!$ cycles primaires; au nombre a_{p+1} d'entre eux, nous donnerons la propriété A. Quant aux autres, nous les décomposerons en cycles secondaires et nous aurons $b_1 P_p(b_1, b_2, \ldots b_p)$ décompositions en cycles secondaires, jouissant tous de la propriété B. Il faut donc que

$$a_{p+1} + b_1 P_p(b_1, b_2, \ldots b_p) \leq p!, \qquad (p = 0, 1, 2, \ldots).$$

Or $b_1 = 1$, donc $a_1 = a_2 = 0$

$$a_3 + b_2 \leq 1, \quad a_4 + 3\, b_2 + b_3 \leq 5, \ldots$$

Ces inégalités étant supposées vérifiées, on a

$$R_{n+1}(\lambda a, b) = \sum_{\mu=0}^{\mu=n} \left[\binom{n}{\mu} a_{\mu+1} R_{n-\mu}\{(\lambda-1)a, b\} + \binom{n}{\mu} b_1 P_\mu(b) R_{n-\mu}(\lambda a, b) \right],$$

d'où la fonction génératrice

$$\varrho_\lambda(z) = \sum_{n=0}^{\infty} R_n(\lambda a, b) \frac{z^n}{n!} = \frac{[a(z)]^\lambda}{\lambda!} e^{\int_0^z e^{b(z)} dz}. \tag{25}$$

26. Soit ensuite $S_n(b, \lambda a)$ le nombre des substitutions de n lettres, dont λ cycles primaires exactement $C', C'', \ldots C^{(\lambda)}$, engendrent des cycles secondaires jouissant de la propriété A et dont tous les autres cycles primaires jouissent de la propriété B. On a maintenant $a_1 = 1$, $b_1 = 0$ et on verra, comme tout à l'heure, que

$$b_{p+1} + P_p(a_1, a_2, \ldots a_p) \leq p!, \qquad (p = 0, 1, 2 \ldots).$$

Si ces conditions sont vérifiées, on établit l'équation récurrente

$$S_{n+1}(b, \lambda a) = \sum_{\mu=0}^{\mu=n} \left[\binom{n}{\mu} a_1 P_\mu(a) S_{n-\mu}\{b, (\lambda-1)a\} + \binom{n}{\mu} b_{\mu+1} S_{n-\mu}(b, \lambda a) \right],$$

d'où l'on tire la fonction génératrice

$$\sigma_\lambda(z) = \sum_{n=0}^{\infty} S_n(b, \lambda a) \frac{z^n}{n!} = \frac{1}{\lambda!} \left[\int_0^z e^{a(z)} dz \right]^\lambda e^{b(z)}. \tag{26}$$

27. Les deux questions traitées aux numéros 25 et 26 conduisent à se demander si les substitutions de n lettres, dont tous les cycles primaires jouissent d'une certaine propriété A, peuvent être considérées comme des substitutions, dont tous les cycles secondaires jouissent d'une propriété B et inversement. En d'autres termes, à un tableau A de cycles primaires, peut-on faire correspondre un tableau B de cycles secondaires et inversement, ces deux tableaux satisfaisant, l'un et l'autre, à la condition d'équipartition des propriétés A et B entre toutes les combinaisons d'un même nombre de lettres, condition que nous avons posée au commencement de ce mémoire?

Pour le savoir, écrivons l'équation

$$e^{b_1 \int_0^z e^{b(z)}\, dz} = e^{a(z)},$$

prenons les logarithmes et différentions; nous aurons

$$a'(z) = b_1 e^{b(z)} \tag{27}$$

d'où

$$a_\nu = b_1 P_{\nu-1}(b_1, b_2, \ldots b_{\nu-1}).$$

Cette formule montre que, les b_ν étant donnés, on en déduira toujours des valeurs admissibles pour les a_ν, car, d'une part, son second membre est essentiellement positif, d'autre part, il est $\leq (\nu - 1)!$, puisque P_ν est un certain nombre de substitutions de ν lettres. De plus, comme $b_1 = 1$, on a $a_\nu \geq 1$ et il existera, dans le tableau A, au moins autant de cycles primaires de chaque ordre qu'il y a de combinaisons du même ordre.

En conséquence, à un tableau B de cycles secondaires, on peut toujours faire correspondre un tableau A de cycles primaires, tel que les substitutions, dont tous les cycles secondaires appartiennent au tableau B, soient aussi celles dont les cycles primaires appartiennent au tableau A.

Mais la proposition inverse n'a pas toujours lieu. On tire en effet de (27)

$$b(z) = \log a'(z) = \log\left(1 + \frac{z}{1} + \frac{a_3 z^2}{2!} + \frac{a_4 z^3}{3!} + \cdots\right),$$

car on a nécessairement $a_1 = a_2 = 1$. Soit

$$\log a'(z) = \frac{z}{1} + \sum_{\nu=2}^{\infty} f_\nu(a_3, a_4, \ldots a_{\nu+1}) \frac{z^\nu}{\nu!},$$

les polynômes f_ν pouvant être formés de proche en proche. On aura

$$b_\nu = f_\nu(a_3, a_4, \ldots a_{\nu+1});$$

or, ces polynômes f_ν peuvent prendre des valeurs négatives et des valeurs supérieures à $(\nu - 1)!$, inadmissibles pour a_ν, qui représente un certain nombre de substitutions circulaires de ν lettres.

A un tableau A de cycles primaires, on ne peut donc pas toujours faire correspondre un tableau B de cycles secondaires. On ne le peut que si la valeur numérique du polynôme $f_\nu(a_3, a_4, \ldots a_{\nu+1})$ reste constamment comprise entre 0 et $(\nu - 1)!$, pour $\nu = 1, 2, 3, \ldots$.

28. Nous ne dirons que quelques mots des cycles tertiaires ou cycles de troisième espèce. On les définira, par rapport aux cycles secondaires, comme nous avons défini ceux-ci, par rapport aux cycles primaires. Si $R_n(a)$ désigne le nombre des substitutions de n lettres, dont tous les cycles tertiaires possèdent une propriété A, on aura

$$R_{n+1}(a) = \sum_{\mu=0}^{\mu=n} \binom{n}{\mu} a_1\, Q_\mu(a)\, R_{n-\mu}(a),$$

$Q_\mu(a)$ ayant la même signification qu'au numéro 21, d'où l'on déduira des polynômes indicateurs de cycles tertiaires.

Pour écrire commodément l'expression de la fonction génératrice de ces polynômes, désignons par Ω une opération telle que, $u(z)$ étant une fonction quelconque de z, on ait

$$\Omega[u(z)] = e^{a_1 \int_0^z u(z)\, dz}$$

Alors, les fonctions génératrices relatives aux indicateurs de cycles de première, de deuxième et de troisième espèces, possédant la propriété A, sont respectivement

$$e^{a(z)}, \ \Omega[e^{a(z)}] \text{ et } \Omega_2[e^{a(z)}],$$

Ω_2 étant l'opération itérée de Ω. En suivant la même marche, on aurait, relativement aux cycles de p-ème espèce, la fonction génératrice $\Omega_{p-1}[e^{a(z)}]$, qui, d'après sa signification même, tend vers la limite $1/(1 - z)$, quand p grandit indéfiniment.

§ VI.

Sur certaines catégories de cycles primaires.

29. Dans les paragraphes précédents, nous nous sommes posés, a priori, certains problèmes relatifs aux cycles primaires ou secondaires des substitutions de n lettres; dans chaque cas, nous avons introduit une fonction génératrice des nombres de substitutions, répondant à la question posée et les formules de récurrence, propres au calcul de ces nombres, que nous avons établies, nous ont constamment conduits, pour ces fonctions génératrices, à des équations différentielles linéaires du premier ordre, s'intégrant immédiatement par de simples quadratures.

Nous abordons maintenant un problème plus difficile et tout différent, qui s'énonce ainsi: étant donnée une série entière

$$P(z) = \sum_{n=0}^{\infty} P_n \frac{z^n}{n!}, \tag{28}$$

satisfaisant à une équation différentielle linéaire du second ordre, de la forme,

$$P''(z) = a'(z) P'(z) + b''(z) P(z), \tag{29}$$

dans laquelle $a(z)$ et $b(z)$ sont des fonctions génératrices de cycles, relatives à des propriétés A et B, et où les accents sont des indices de dérivation, interpréter le nombre P_n, comme dénombrant les substitutions de n chiffres, qui appartiennent à certaines familles à définir.

Remarquons tout de suite, pour ne plus y revenir, qu'il n'est pas nécessaire ici que les propriétés A et B s'excluent mutuellement. Les cycles, auxquels elles s'appliqueront respectivement, se différencieront par leur nature même, comme nous le verrons plus loin, et indépendamment de ce que peuvent être les propriétés A et B. La série $a(z) + b(z)$ est majorée par $-2 \log(1-z)$ et non pas nécessairement par $-\log(1-z)$. La fonction $P(z)$ reste ce que nous avons appelé une fonction génératrice de substitutions, même pour $a(z) = b(z) = -\log(1-z)$ et engendre, dans ce cas, le nombre des substitutions du groupe symétrique tout entier.

Pour plus de clarté, nous exposerons d'abord l'interprétation que nous avons obtenue des nombres P_n et nous donnerons ensuite la démonstration. Nous n'aurons affaire, dans tout ce paragraphe, qu'à des cycles primaires.

Les n chiffres permutés par une substitution S étant $1, 2, 3, \ldots n$, décomposons S en cycles et appelons »hauteur» d'un cycle le chiffre le plus faible qu'il contienne; rangeons les cycles de S, de gauche à droite, par ordre de hauteurs croissantes, de sorte que

$$S = C_1\, C_\alpha\, C_\beta \ldots . C_\eta\, C_\theta\, C_\zeta \ldots C_\lambda\, C_\mu\, C_\nu, \tag{30}$$

$$1 < \alpha < \beta < \ldots < \eta < \theta < \ldots < \mu < \nu.$$

Les indices des cycles sont ici leurs hauteurs respectives et n'ont rien à voir avec leur ordre; le chiffre le plus faible que contienne le cycle C_α est α et C_α contient sûrement le chiffre α.

1 et 2 sont les deux chiffres les plus faibles, parmi les n chiffres que permute S; nous désignerons par α et α' les deux chiffres les plus faibles parmi ceux que permute S, une fois qu'on en a exclus les chiffres permutés par le cycle C_1, c'est-à-dire les deux chiffres les plus faibles, parmi ceux que permute $S C_1^{-1}$; nous désignerons par β et β' les deux chiffres les plus faibles, parmi ceux que permute $S C_1^{-1} C_\alpha^{-1}$, et ainsi de suite. Nous dirons alors qu'un cycle C_θ, par exemple, appartient à la catégorie K_1, s'il ne contient pas θ' et à la catégorie K_2, s'il contient θ'. Le dernier cycle à droite de (30), savoir C_ν, est donc de catégorie K_2, car il contient forcément ν', sauf si C_ν est d'ordre 1, auquel cas il est de catégorie K_1.

Ces conventions admises, il est nécessaire de préciser les conditions initiales déterminant l'intégrale (28) de notre équation différentielle (29). Nous prendrons d'abord $P_0 = 1$ et $P_1 = a_1$. Dans ces conditions, nous allons démontrer que P_n est égal au nombre des substitutions de n chiffres, dont tous les cycles de catégorie K_1 possèdent la propriété A et dont tous les cycles de catégorie K_2 possèdent la propriété B. Nous dirons, pour abréger, qu'un cycle est K_1, s'il appartient à la catégorie K_1 et de même pour K_2.

La démonstration de cette proposition repose simplement sur la lecture attentive de la formule de récurrence

$$\begin{aligned} P_{n+2} = {} & a_1 P_{n+1} + \binom{n}{1} a_2 P_n + \binom{n}{2} a_3 P_{n-1} + \cdots + a_{n+1} P_1 \\ & + b_2 P_n + \binom{n}{1} b_3 P_{n-1} + \binom{n}{2} b_4 P_{n-2} + \cdots + b_{n+2} P_0, \end{aligned} \tag{31}$$

qui découle de (29) et que nous avons écrite, à dessein, sur deux lignes.

Nous supposerons que les chiffres permutés dans P_{n+2} sont $1, 2, 3, \ldots n+2$ et que ceux, permutés dans P_{n+2-i} sont $i+1, i+2, \ldots. n+1, n+2$; de sorte que le dernier chiffre introduit, dans les substitutions dénombrées ou symbolisées par P_μ, (suivant que l'on considère P_μ comme un nombre ou comme un symbole indicateur de cycles), est le chiffre 1 et non pas, comme nous l'avions fait dans les paragraphes précédents, le chiffre μ. Il n'y a là qu'un simple changement de notations.

L'équation (31) nous montre comment, pour former P_{n+2}, on doit associer le dernier chiffre introduit, 1, aux chiffres précédemment introduits, $2, 3, \ldots n+1$, $n+2$, qui ont servi à former P_{n-1}, P_n, $P_{n+1}, \ldots.$ En nous référant à l'expression (30), cette équation (31) nous montre comment on forme le cycle de plus faible hauteur, savoir le cycle C_1.

Nous voyons, par le premier terme à gauche de la première ligne, que l'on a d'abord pris le chiffre 1 tout seul, pour en faire un cycle unité, qui est un cycle A, puisque son symbole est a_1. La condition initiale, $P_1 = a_1$, que nous avons admise, est donc nécessaire; a_1 peut être égal à 0 ou à 1, mais il faut que $P_1 = a_1$. Les deuxième, troisième, ... termes de la première ligne montrent qu'on a successivement associé, dans des cycles, le chiffre 1 non pas à des combinaisons des $n+1$ chiffres restants, mais à des combinaisons de ces chiffres, après qu'on en a exclus un chiffre, le chiffre 2. Ces cycles sont des cycles K_1 et on leur a donné la propriété A.

La seconde ligne de (31) montre qu'on a pris le couple 1, 2, contenant le chiffre 2, exclus de la première ligne, pour associer 1 et 2, dans des cycles, aux diverses combinaisons des chiffres restants, $3, 4, 5, \ldots n+2$. Ces cycles sont donc des cycles K_2 et on leur a donné la propriété B.

Nous avons ainsi formé le premier cycle à gauche, C_1, de l'expression (30), mais il faut que la même loi de formation ait été respectée, lors de la formation des autres cycles de la substitution S. Or, d'après la définition que nous avons donnée des catégories K_1 et K_2, c'est bien ce qui a lieu, car nous avons pris soin de ranger les cycles de S par ordre de hauteurs croissantes et, dans le cycle C_α, ce sont les deux chiffres α et α', qui jouent, par rapport à l'ensemble des chiffres que permute la substitution SC_1^{-1}, le même rôle que les chiffres 1 et 2, par rapport à l'ensemble des chiffres que permute la substitution S. Le cycle C_α a donc été formé suivant la même loi que C_1. De même, β et β' étant les deux plus faibles chiffres dans l'ensemble de chiffres que permute $SC_1^{-1}C_\alpha^{-1}$, le cycle C_β a, lui aussi, été formé suivant la même loi que C_1 et C_α. Et ainsi de suite. Notre proposition est donc démontrée.

30. Nous l'avons énoncée sous une forme susceptible d'être étendue immédiatement aux équations différentielles du troisième ordre ou d'ordre supérieur, mais, dans le cas actuel d'une équation du second ordre, on peut définir plus simplement les catégories K_1 et K_2. Si, en nous reportant à (30), le cycle C_η est K_1, il ne contient pas η' et, par conséquent, θ, hauteur du cycle C_θ, voisin de droite de C_η, sera égal à η'. Si, au-contraire, C_η est K_2, il contient η' et l'on aura $\theta > \eta'$. D'où la définition très simple:

Un cycle est K_1, s'il ne contient qu'un seul chiffre inférieur à la hauteur du cycle placé immédiatement à sa droite; un cycle est K_2, s'il contient au moins deux chiffres inférieurs à la hauteur du cycle placé immédiatement à sa droite. De plus, le dernier cycle à droite est toujours K_2, sauf s'il ne contient qu'un seul chiffre, auquel cas il est K_1.

31. Reste à interpréter P_n, lorsque les conditions initiales sont $P_0 = 0$ et $P_1 = a_1$. La deuxième ligne de (31) montre alors qu'on supprime le terme $b_{n+2} P_0$, c'est-à-dire qu'après avoir formé le cycle C_1, cycle de plus faible hauteur d'une substitution S, on doit le rejeter lorsqu'il contient toutes les lettres permutées par S, donc lorsque S est circulaire. Il y a exception, toutefois, si S ne permute qu'une seule lettre; la deuxième ligne de (31) ne contient pas, en effet, le coefficient b_1, symbole d'un cycle unité et, par suite, la formule ne prescrit pas d'exclure une substitution circulaire, lorsqu'elle est d'ordre 1. En d'autres termes, dans l'hypothèse $P_0 = 0$, la substitution S n'est pas circulaire, à moins de se réduire à un cycle unité. Une règle analogue a dû être observée, lors de la formation des autres cycles de S; donc $S\,C_1^{-1}$ n'est pas circulaire, à moins de se réduire à un cycle unité; de même pour $S\,C_1^{-1}\,C_\alpha^{-1}, \ldots$ Finalement, les catégories K_1 et K_2 sont définies comme précédemment, mais toute substitution S, dans laquelle le cycle C_ν, de plus grande hauteur, est d'ordre supérieur à l'unité, doit être rejetée.

32. Les explications détaillées que nous avons données au-sujet de l'équation (29) nous permettront d'être beaucoup plus brefs, pour les équations du troisième ordre. Elles sont de deux types distincts, le premier d'entre eux étant

$$P'''(z) = a'(z)\,P''(z) + 2\,b''(z)\,P'(z) + b'''(z)\,P(z), \tag{32}$$

où chacune des séries $a(z), b(z), c(z)$ est majorée par $-\log(1-z)$ et où leur somme est majorée par $-3\log(1-z)$. L'équation (32) entraîne la formule récurrente

$$(33)\qquad \begin{aligned} P_{n+3} = {} & a_1 P_{n+2} + \binom{n}{1} a_2 P_{n+1} + \cdots + a_{n+1} P_2 \\ & + 2\left[b_2 P_{n+1} + \binom{n}{1} b_3 P_n + \cdots + b_{n+2} P_1\right] \\ & + c_3 P_n + \binom{n}{1} c_4 P_{n-1} + \cdots + c_{n+3} P_0. \end{aligned}$$

En revenant à l'expression (30) d'une substitution S, les cycles de S se répartissent en trois catégories définies comme suit. Soient 1, 2, 3 les trois plus faibles chiffres permutés par S; α, α', α'', les trois plus faibles chiffres permutés par $S\,C_1^{-1}$, ... $\theta, \theta', \theta''$, les trois plus faibles chiffres permutés par $S\,C_1^{-1}\,C_\alpha^{-1}\ldots C_\eta^{-1}$, et ainsi de suite; le cycle C_θ est un cycle K_1, s'il ne contient ni θ', ni θ''; c'est un cycle K_2, s'il contient θ' ou θ'', mais non pas θ' et θ''; c'est un cycle K_3, s'il contient θ' et θ''. Le cycle de plus grande hauteur C_ν est toujours un cycle K_3, à moins qu'il ne contienne que deux chiffres et c'est alors un cycle K_2, ou à moins qu'il ne contienne qu'un seul chiffre et c'est alors un cycle K_1.

Examinons les conditions initiales. On peut avoir $P_0 = 0$ ou $P_0 = 1$. On a nécessairement, comme pour (29), et pour la même raison, $P_1 = a_1$. Autrement dit, un cycle d'une lettre est A. D'après le premier terme de la seconde ligne de (33), un cycle d'ordre 2, s'il est K_2, est nécessairement un cycle B. D'autre part, P_2, considéré comme un indicateur de cycles, peut contenir un terme en a_1^2, qui représente deux cycles unités A; mais P_2 ne peut pas contenir de terme en b_1^2, puisqu'un cycle unité est A. P_2 ne peut pas non plus contenir de terme a_2, car le cycle de plus grande hauteur peut être d'ordre 2 et c'est alors un cycle K_2; or comme nous venons de le voir, un cycle K_2, d'ordre 2, est un cycle B. On peut donc avoir soit $P_2 = a_1^2$, soit $P_2 = b_2$, soit $P_2 = a_1^2 + b_2$.

Prenons les conditions initiales $P_0 = 1$, $P_1 = a_1$, $P_2 = a_1^2 + b_2$; alors P_n est le nombre des substitutions du groupe symétrique de n chiffres, dans lesquelles tous les cycles K_1 sont A, tous les cycles K_2 sont B et tous les cycles K_3 sont C.

33. Si l'on fait $P_0 = 0$, on verra, par l'examen du dernier terme à droite de la troisième ligne de (33) et en raisonnant comme nous l'avons fait pour l'équation (29), que toute substitution S, dans laquelle le cycle de plus grande hauteur est d'ordre supérieur à 2, doit être rejetée.

Faisons $P_2 = b_2$; nous écartons donc le terme a_1^2, qui représente deux cycles unités. En examinant le dernier terme de la première ligne de (33) et en appliquant ce principe que tout raisonnement fait sur la substitution S, tout entière, doit être répété sur les substitutions antérieurement formées, $S\,C_1^{-1}$, $S\,C_1^{-1}\,C_\alpha^{-1}, \ldots$, nous concluerons que si C_λ, C_μ, C_ν sont les trois cycles de plus grande hauteur de S, $\lambda < \mu < \nu$, et si, C_λ étant K_1, C_μ et C_ν sont tous deux d'ordre 1, la substitution S doit être rejetée. En d'autres termes, si l'expression (30) se termine à droite par $C_\lambda\,C_{\lambda'}\,C_{\lambda''}$, où λ' et λ'' sont, comme il a été convenu, les deux plus faibles chiffres, supérieurs à λ, parmi les chiffres que permute ce groupe de trois cycles, et si $C_{\lambda'}$ et $C_{\lambda''}$ sont d'ordre 1, la substitution S doit être rejetée.

Faisons, enfin $P_2 = a_1^2$. Alors, si les deux cycles de plus grande hauteur d'une substitution S sont C_μ et C_ν, $\mu < \nu$, C_μ étant un cycle K_1 et C_ν un cycle d'ordre 2, S doit être rejetée. Pour qu'il en soit ainsi, il suffit que $\nu = \mu'$ et que C_ν soit d'ordre 2.

34. Le deuxième type d'équation différentielle du troisième ordre est

$$P'''(z) = a'(z)\,P''(z) + b''(z)\,P'(z) + c'''(z)\,P(z). \tag{34}$$

Avec les notations du numéro 32, un cycle quelconque C_θ est K_1, s'il ne contient ni θ', ni θ''; il est K_2, s'il contient θ' et non θ''; il est K_3, s'il contient θ' et θ''. Dans le cas actuel, cette définition peut être simplifiée. Soit C_ζ le cycle situé immédiatement à droite de C_θ; alors C_θ est K_1, s'il contient exactement un chiffre inférieur à ζ et alors $\zeta = \theta'$; il est K_2, s'il contient exactement deux chiffres inférieurs à ζ, et alors $\zeta = \theta''$; il est K_3, s'il contient au moins trois chiffres inférieurs à ζ.

L'interprétation du nombre P_n est la même que pour l'équation (32) et les diverses conditions initiales s'interprètent aussi de la même façon.

Il y a lieu de remarquer que, pour $a_\nu = b_\nu = c_\nu = (\nu - 1)!$, $(\nu = 1, 2, 3, \ldots)$ c'est-à-dire pour $a(z) = b(z) = c(z) = -\log(1 - z)$, aucune intégrale de l'équation (34) n'engendre, par son développement en série, la totalité des substitutions du groupe symétrique. Effectivement aucun cycle C_θ, contenant les chiffres θ et θ'', sans contenir le chiffre θ' n'a été formé. Un tel cycle n'appartient à aucune des catégories K_1, K_2, K_3, que définit l'équation différentielle (34). En conséquence, si une substitution S contient un cycle de cette nature, elle doit être rejetée.

35. Les équations du quatrième ordre seront de neuf types différents,

$$P^{(4)}(z) = a'(z)\,P'''(z) + g\,b''(z)\,P''(z) + h\,c'''(z)\,P'(z) + d^{(4)}(z)\,P(z),$$

les coefficients g et h pouvant chacun prendre les valeurs 1, 2 ou 3. Seule l'équation correspondant à $g = h = 3$ aura, pour

$$a(z) = b(z) = c(z) = d(z) = -\log(1 - z),$$

une intégrale engendrant tout le groupe symétrique. La définition des catégories de cycles K_1, K_2, K_3 et K_4 s'obtiendra par une généralisation évidente de ce qui a été fait pour les équations du deuxième et du troisième ordre. Les conditions initiales seront:

$P_0 = 0$ ou $P_0 = 1$,

$P_1 = a_1$,

$P_2 = a_1^2 + b_2$ ou $P_2 = a_1^2$ ou $P_2 = b_2$,

$P_3 = a_1^3 + 3\,a_1 b_2 + c_3$ ou $P_3 = a_1^3$ ou $P_3 = 3\,a_1 b_2$ ou $P_3 = c_3$ ou $P_3 = a_1^3 + 3\,a_1 b_2$ ou $P_3 = a_1^3 + c_3$ ou $P_3 = 3\,a_1 b_2 + c_3$.

En tout, il y aura 42 systèmes distincts de conditions initiales. Comme l'équation différentielle ne possède que quatre intégrales indépendantes, il existera des relations linéaires entre les nombres P_n correspondant à 5 systèmes différents de conditions initiales. Une remarque analogue s'applique déjà au cas de l'équation du troisième ordre, pour laquelle il existe trois intégrales indépendantes et six systèmes différents de conditions initiales.

36. Considérons l'équation différentielle

$$u''(z) = e^z u(z). \tag{35}$$

Le coefficient u_n de l'intégrale

$$\sum_{n=0}^{\infty} u_n \frac{z^n}{n!},$$

pour laquelle $u_0 = 1$ et $u_1 = 0$, est égal au nombre des substitutions de n lettres, qui n'ont aucun cycle de catégorie K_1 et dont tous les cycles de catégorie K_2 sont monotones.

L'équation (35) donne d'abord une formule de récurrence qui s'écrit, sous forme symbolique,

$$u_{n+2} = (u + 1)^n.$$

De plus, si, dans (35), on fait le changement de variable $e^z = x$ et le changement de fonction $u(z) = v(x)$, la transformée est une équation de Bessel

$$x\,v''(x) + v'(x) - v(x) = 0.$$

Les intégrales en sont bien connues; en y remplaçant x par e^z et en développant les exponentielles, on obtient l'expression des nombres u_n au moyen des belles séries infinies suivantes. Soit

$$s_n = \sum_{\nu=0}^{\infty} \frac{\nu^n}{(\nu!)^2},$$

$$\sigma_n = \sum_{\nu=1}^{\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{\nu}\right) \frac{\nu^n}{(\nu!)^2},$$

on a

$$u_n = s_0 s_n - n s_1 s_{n-1} + 2(s_1 \sigma_n - \sigma_1 s_n).$$

Cette équation, qui permet d'exprimer σ_n en fonction linéaire de s_n, de s_{n-1} et du nombre entier u_n, se réduit, pour $n = 0$, à une relation connue; mais, pour $n > 0$, il semble qu'elle soit nouvelle.

37. Indiquons encore le résultat suivant: les catégories K_1 et K_2 étant celles qui sont relatives à une équation du second ordre, le nombre S_n des substitutions paires de n chiffres et le nombre T_n des substitutions impaires de n chiffres, dont tous les cycles K_1 ont la propriété A et dont tous les cycles K_2 ont la propriété B, ont respectivement pour fonctions génératrices

$$\sum_{n=0}^{\infty} S_n \frac{z^n}{n!} = \frac{\sigma(z) + \tau(-z)}{2},$$

$$\sum_{n=0}^{\infty} T_n \frac{z^n}{n!} = \frac{\sigma(z) - \tau(-z)}{2},$$

où $\sigma(z)$ et $\tau(z)$ sont respectivement les intégrales des équations

$$\sigma''(z) = a'(z)\sigma'(z) + b''(z)\sigma(z),$$
$$\tau''(z) = -a'(z)\tau'(z) - b''(z)\tau(z),$$

satisfaisant aux conditions initiales

$$\sigma(0) = 1, \qquad \sigma'(0) = a_1,$$
$$\tau(0) = 1, \qquad \tau'(0) = -a_1.$$

§ VII.

Applications diverses.

38. Les applications qui suivent s'obtiennent facilement par la considération des polynômes indicateurs de cycles. Soit $\Gamma_n(a_1, a_2, \ldots\ b_1, b_2, \ldots\ c_1, c_2, \ldots)$

ou, plus brièvement, $\Gamma_n(a, b, c)$ l'un de ces polynômes, relatif aux substitutions de n lettres, dont les cycles, qui peuvent être des cycles primaires ou secondaires ou d'espèce plus élevée, possèdent des propriétés A, B ou C. Les divers termes de Γ_n sont de la forme

$$T_\lambda = M_\lambda a_1^{\alpha_1} \dots a_i^{\alpha_i} \dots b_1^{\beta_1} \dots b_j^{\beta_j} \dots c_1^{\gamma_1} \dots c_k^{\gamma_k} \dots,$$

M_λ étant un certain coefficient numérique. Le nombre des cycles d'ordre i, jouissant de la propriété A, dans les substitutions semblables entre elles, représentées par T_λ, est évidemment $a_i \partial T_\lambda / \partial a_i$ et, par suite, le nombre $\nu(n, i, a)$ des cycles A, d'ordre i, dans les substitutions de n lettres, représentées par Γ_n est

(36) $$\nu(n, i, a) = a_i \frac{\partial \Gamma_n}{\partial a_i}.$$

Supposons, en particulier, qu'il s'agisse de cycles primaires et que la fonction génératrice de Γ_n soit de la forme

(37) $$F[a(z), b(z), c(z)] = \sum_{n=0}^{\infty} \Gamma_n(a, b, c) \frac{z^n}{n!};$$

désignons respectivement par F_1, F_2 et F_3 les dérivées partielles de la fonction $F(u, v, w)$, par rapport à u, v et w. On aura, d'après (36),

$$F_1[a(z), b(z), c(z)] \, a_i \frac{z^i}{i!} = \sum_{n=0}^{\infty} \nu(n, i, a) \frac{z^n}{n!},$$

puisque $\partial a(z) / \partial a_i = z^i / i!$ et le nombre total

(38) $$\nu(n, a) = \sum_{i=1}^{i=n} \nu(n, i, a)$$

des cycles jouissant de la propriété A, dans les substitutions représentées par Γ_n, aura pour fonction génératrice

(39) $$\sum_{n=0}^{\infty} \nu(n, a) \frac{z^n}{n!} = a(z) F_1[a(z), b(z), c(z)].$$

Il est clair, en effet, que les termes en z^{n+1}, z^{n+2}, ... dans le facteur $a(z)$ du second membre, n'influent pas sur le coefficient $\nu(n, a)$ au premier membre.

D'une manière analogue, la somme

(40) $$\sigma(n, a) = \sum_{i=1}^{i=n} i\,\nu(n, i, a)$$

aura pour fonction génératrice

(41) $$\sum_{n=0}^{\infty} \sigma(n, a) \frac{z^n}{n!} = z\,a'(z)\,F_1[a(z), b(z), c(z)].$$

Nous définirons l'ordre moyen $\mu(n, a)$ de tous les cycles, jouissant de la propriété A, dans les substitutions représentées par Γ_n, par la formule

(42) $$\sigma(n, a) = \mu(n, a)\,\nu(n, a).$$

$\mu(n, a)$ est donc le quotient du terme en z^n, dans le développement (41), par le terme en z^n, dans le développement (39).

L'ordre moyen $\mu(n)$ de tous les cycles primaires, dans les substitutions représentées par Γ_n, qu'ils soient indifféremment des cycles A, des cycles B ou des cycles C, serait défini par

$$\sigma(n, a) + \sigma(n, b) + \sigma(n, c) = \mu(n)\,[\nu(n, a) + \nu(n, b) + \nu(n, c)].$$

Si le polynôme indicateur Γ_n est relatif à des cycles d'espèce supérieure à la première, le calcul ci-dessus devra être modifié, parce que la fonction génératrice de Γ_n n'affectera certainement plus la forme (37), mais la formule (36) reste valable dans tous les cas.

39. Dans le groupe symétrique de degré n, on a $a(z) = -\log(1 - z)$, $b(z) = c(z) = 0$, et le nombre total des cycles primaires est, d'après ce qui précède,

$$\nu(n) = n!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right);$$

d'autre part

$$\sigma(n) = n \cdot n!,$$

de sorte que l'ordre moyen d'un cycle est

$$\mu(n) = \frac{n}{1 + \frac{1}{2} + \cdots + \frac{1}{n}} \sim \frac{n}{\log n},$$

le signe $\sim$ signifiant une égalité asymptotique et il nous semble bien remarquable que l'expression du troisième membre soit, elle-même, asymptotique au nombre des nombres premiers, inférieurs ou égaux à n.

Désignons par $\nu'(n,i), \nu'(n), \sigma'(n), \mu'(n)$, les nombres, définis comme $\nu(n,i)$, $\nu(n), \sigma(n), \mu(n)$, mais relatifs aux cycles secondaires. En ayant recours à (36) et en se rappelant la formule (18) du § V, on démontre facilement que

$$\nu'(n,1) = n! + 2(n!)\left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right)$$

et que, pour $i = 2, 3, \ldots n-1$,

$$\nu'(n,i) = \frac{n!}{i}\left(\frac{1}{i+1} + \frac{1}{i+2} + \cdots + \frac{1}{n}\right),$$

car il n'y a pas de cycles secondaires d'ordre n, dans les substitutions de degré n. Après quelques calculs, on trouve alors

$$\sigma'(n) = n \cdot n!$$
$$\nu'(n) = n!\,\gamma_1(n) + n!\,\gamma_2(n),$$

où $\gamma_1(n)$ et $\gamma_2(n)$ désignent respectivement les coefficients de x et de x^2, dans le développement de

$$\left(1+\frac{x}{1}\right)\left(1+\frac{x}{2}\right)\cdots\left(1+\frac{x}{n}\right) = 1 + \gamma_1(n)x + \gamma_2(n)x^2 + \cdots$$

L'ordre moyen des cycles secondaires des substitutions de n lettres est, par suite,

$$\mu'_n = \frac{n}{\gamma_1(n) + \gamma_2(n)}$$

et son expression asymptotique s'obtient en remarquant que, pour $n = \infty$,

$$\frac{1}{\Gamma(x+1)} = n^{-x}\left[1 + \gamma_1(n)x + \gamma_2(n)x^2 + \cdots\right] = 1 + Cx + \frac{C^2 - s_2}{2}x^2 + \cdots,$$

où $s_2 = \pi^2/6$ et où C est la constante d'Euler. On a ainsi

$$\mu'(n) \sim \frac{2n}{\log^2 n + 2(1+C)\log n},$$

de sorte que le quotient de l'ordre moyen des cycles primaires par l'ordre moyen des cycles secondaires, dans le groupe symétrique de degré n, augmente asymptotiquement comme $\log\sqrt{n}$.

On observera que $\sigma'(n) = \sigma(n)$. Or, les cycles tertiaires sont dans le même rapport avec les cycles secondaires que ceux-ci avec les cycles primaires; on voit donc, en procédant par induction, que la somme $\sigma(n)$, étendue aux cycles de

p-ème espèce de toutes les substitutions de n lettres, est un invariant; sa valeur constante, indépendante de p, est $n \cdot n!$.

40. En généralisant ce qui précède, on pourrait déterminer l'ordre moyen des cycles de p-ème espèce. Bornons-nous à donner les éléments du calcul à effectuer. Soit $\nu_p(n, i)$ le nombre des cycles de p-ème espèce et d'ordre i, contenus dans toutes les substitutions du groupe symétrique de degré n et soit

$$\varphi_p(z, i) = \sum_{n=0}^{\infty} \nu_p(n, i) \frac{z^n}{n!}$$

la fonction génératrice de ce nombre. D'après le numéro 28 du § V, on aura

$$\varphi_p(z, i) = a_i \frac{\partial}{\partial a_i} \{\Omega_{p-1}[e^{a(z)}]\},$$

si, dans le second membre et après différentiation, on pose $a_i = (i-1)!$, c'est-à-dire $a(z) = -\log(1-z)$. Il y a alors à distinguer le cas des cycles du premier ordre, $i = 1$, de celui des cycles d'ordre supérieur au premier, $i \geq 2$.

Pour le premier ordre, $\nu_p(n, 1)$ est le coefficient de x^{p-1} dans le développement de Maclaurin de l'expression

$$\frac{1}{1-x}[2(2+x)(3+x)\cdots(n+x) - n!].$$

Pour l'ordre $i \geq 2$, on a:
si $n < i$, $\nu_p(n, i) = 0$, $(p = 1, 2, 3, \ldots .)$;
si $n = i$, $\nu_1(i, i) = (i-1)!$ et $\nu_p(i, i) = 0$, $(p = 2, 3, 4, \ldots)$;
si $n > i$, $\nu_p(n, i)$ est le coefficient de x^{p-1}, dans le développement de l'expression

$$(i-1)!(i+1+x)(i+2+x)\ldots(n+x).$$

De plus, $\nu_p(n, i)$ est nul si $n \leq p$.

41. Indiquons encore qu'à l'aide de la première équation (13) du § III, on trouve, pour le nombre $\alpha(n)$ de tous les cycles primaires contenus dans les substitutions du groupe alterné de n lettres, la valeur

$$\alpha(n) = \frac{n!}{2}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) + (-1)^n \frac{(n-2)!}{2};$$

on en déduit immédiatement le nombre de tous les cycles des substitutions impaires, puisqu'on connaît le nombre total des cycles contenus dans le groupe symétrique.

42. Comme application du § VI, considérons les cycles K_1 et K_2, définies par l'intégrale de l'équation différentielle (29), qui satisfait aux conditions initiales $P(0) = 1$, $P'(0) = a_1$ et cherchons d'abord le nombre P_n des substitutions de n lettres qui ne contiennent pas de cycle K_2 et dont les cycles K_1 sont quelconques. Il suffit, dans (29), de faire $b(z) = 0$, $a(z) = -\log(1-z)$, pour trouver $P(z) = 1 - \log(1-z)$, d'où $P_n = (n-1)!$.

On aura de même le nombre Q_n des substitutions de n lettres, qui ne contiennent pas de cycle K_1 et dont les cycles K_2 sont quelconques, en intégrant l'équation $Q''(z) = (1-z)^{-2} Q(z)$, avec $Q(0) = 1$, $Q'(0) = 0$. On trouve ainsi

$$(-1)^n Q_n = \frac{\beta}{\beta-\alpha}\alpha(\alpha-1)\ldots(\alpha-n+1) + \frac{\alpha}{\alpha-\beta}\beta(\beta-1)\ldots(\beta-n+1),$$

où α et β sont les racines de $\alpha^2 - \alpha - 1 = 0$. Pour le calcul des nombres P_n, on se servira plus commodément de la formule de récurrence

$$Q_{n+2} = 2n\, Q_{n+1} - (n^2 - n - 1) Q_n,$$
$$Q_0 = 1,\ Q_1 = 0,\ Q_2 = 1,\ Q_3 = 2,\ Q_4 = 7, \ldots$$

Enfin, le nombre des substitutions de n lettres, dont les cycles K_1 sont tous du premier ordre et dont les cycles K_2 sont tous du second ordre, est égal à R_n, R_n étant le terme d'indice n de la suite de Fibonacci, $R_0 = 1$, $R_1 = 1$, $\ldots$ $R_n = R_{n-1} + R_{n-2}$.

43. Je cherche maintenant l'ordre moyen des cycles K_1, dans le groupe symétrique de n lettres. Je désignerai par $k_1(n, i)$ le nombre des cycles d'ordre i et par $K_1(z, i)$ sa fonction génératrice

$$K_1(z, i) = \sum_{n=0}^{\infty} k_1(n, i) \frac{z^n}{n!}\cdot$$

Je poserai, de plus,

$$k_1(n) = \sum_{i=1}^{i=n} k_1(n, i),$$

$$\xi_1(n) = \sum_{i=1}^{i=n} i\, k_1(n, i)$$

et l'ordre moyen $X_1(n)$ sera, par définition, le quotient de $\xi_1(n)$ par $k_1(n)$. Les mêmes lettres k, K, ξ et X, affectées de l'indice 2, seront relatives à la catégorie K_2.

Les valeurs initiales des nombres $k_1(n, i)$ sont:

$$\text{pour } i = 1, \quad k_1(1, 1) = 1, \quad k_1(2, 1) = 2,$$
$$\text{pour } i > 1, \quad k_1(1, i) = 0, \quad k_1(2, i) = 0;$$

celles des nombres $k_2(n, i)$ sont:

$$\text{pour } i = 1, \quad k_2(1, 1) = 0, \quad k_2(2, 1) = 0,$$
$$\text{pour } i = 2, \quad k_2(2, 1) = 0, \quad k_2(2, 2) = 1,$$
$$\text{pour } i > 2, \quad k_2(1, i) = 0, \quad k_2(2, i) = 0.$$

Si nous supposons qu'à l'aide de la récurrence, déduite de (29), nous ayons formé l'indicateur de cycles $P_n(a_1, a_2, \ldots b_2, b_3, \ldots)$, nous devrons, pour obtenir $k_1(n, i)$ et en vertu de (36), appliquer l'opérateur $a_i \dfrac{\partial}{\partial a_i}$ à P_n et faire ensuite $a_i = b_i = (i-1)!$. En tenant compte du fait que les opérateurs $\dfrac{d}{dz}$ et $a_i \dfrac{\partial}{\partial a_i}$ sont permutables, on obtient donc la fonction génératrice $K_1(z, i)$ comme l'intégrale de l'équation différentielle

$$K_1''(z, i) - \frac{1}{1-z} K_1'(z, i) - \frac{1}{(1-z)^2} K_1(z, i) = \frac{z^{i-1}}{(1-z)^2}, \tag{43}$$

satisfaisant aux conditions initiales,

$$\text{pour } i = 1, \quad K_1'(0, 1) = 1, \quad K_1''(0, 1) = 2,$$
$$\text{pour } i > 1, \quad K_1'(0, i) = 0, \quad K_1''(0, i) = 0.$$

L'équation sans second membre ayant, pour intégrale générale, $A(1-z) + B(1-z)^{-1}$, la méthode de la variation des constantes A et B donne facilement une intégrale particulière de (43) et l'on obtient ainsi les résultats suivants:

Pour $i = 1$,

$$K_1(z, 1) = \frac{z}{1-z}$$

d'où

$$k_1(n, 1) = n!, \tag{44}$$

ce qui devait être, puisque les cycles unités appartiennent à la catégorie K_1.

Pour $i = 2$,

$$K_1(z, 2) = \frac{1}{4}\frac{3z^2 - 2z}{1-z} + \frac{1}{2}(1-z)\log\frac{1}{1-z},$$

d'où

$$k_1(n, 2) = \frac{1}{4} n! - \frac{1}{2}(n-2)!\cdot$$

Pour $i > 2$,

$$K_1(z, i) = \frac{i-1}{4} \frac{3z^2 - 2z}{1-z} - \frac{i-1}{2}(1-z)\log(1-z)$$
$$- \frac{i-1}{1-z}\left[\frac{z^3}{1\cdot 2\cdot 3} + \frac{z^4}{2\cdot 3\cdot 4} + \cdots + \frac{z^i}{(i-2)(i-1)i}\right],$$

d'où

(45) $$k_1(n, i) = \frac{1}{2i} n! - \frac{i-1}{2}(n-2)!$$

et l'on voit que le cas de $i = 2$ rentre dans le cas général (45).

En partant des égalités (44) et (45), une sommation facile donne alors

$$k_1(n) = \frac{1}{2} n!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) + \frac{1}{4} n!,$$

$$\xi_1(n) = \frac{1}{3}(n+1)!$$

$$X_1(n) = \frac{4}{3} \frac{n+1}{1 + 2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right)}.$$

L'ordre moyen des cycles K_1, dans le groupe symétrique de degré n est donc, asymptotiquement,

$$X_1(n) \sim \frac{2}{3} \frac{n}{\log n}.$$

On aura, de même, pour la catégorie K_2,

$$k_2(n) = \frac{1}{2} n!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) - \frac{1}{4} n!,$$

$$\xi_2(n) = \frac{1}{3} n!\,(2n-1),$$

$$X_2(n) = \frac{4}{3} \frac{2n-1}{2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) - 1},$$

et, asymptotiquement,

$$X_2(n) \sim \frac{4}{3} \frac{n}{\log n}.$$

En nous reportant à l'ordre moyen $\mu(n)$ des cycles de toutes les substitutions, sans distinction de catégorie, nous voyons que $\mu(n)$ est asymptotiquement la moyenne arithmétique de $X_1(n)$ et de $X_2(n)$.

44. Enfin, une méthode analogue à celle du numéro précédent donnerait, pour le nombre total $\alpha_1(n)$ des cycles K_1, contenus dans le groupe alterné de degré n, l'expression

$$\alpha_1(n) = \frac{1}{4} n! \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) + \frac{1}{8} n!$$
$$+ (-1)^n \frac{1}{2} (n-2)! \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{4} - \cdots - \frac{1}{n-2}\right)$$

et, en se reportant au numéro 41, on déterminerait, sans peine, le nombre $\alpha_2(n)$ des cycles K_2 contenus dans le groupe alterné ainsi que les nombres $\beta_1(n)$ et $\beta_2(n)$ des cycles K_1 et K_2, contenus dans l'ensemble des substitutions impaires de n lettres.