Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 25 (1951)

Artikel: Les bases du groupe symétrique dont l'une des substitutions est un cycle du sixième ordre.

Autor: Piccard, Sophie

DOI: https://doi.org/10.5169/seals-20698

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 14.12.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Les bases du groupe symétrique dont l'une des substitutions est un cycle du sixième ordre

Par Sophie Piccard, Neuchâtel

§ 1. Introduction

Soit n un entier ≥ 6, soit $\mathfrak{S}_n$ le groupe symétrique des substitutions des éléments $1, 2, \ldots, n$. Il existe, comme on sait, des couples S, T de substitutions de $\mathfrak{S}_n$ — appelés bases de $\mathfrak{S}_n$ — qui engendrent le groupe $\mathfrak{S}_n$ tout entier par composition finie.

Le but du présent travail est de rechercher toutes les bases S, T du groupe $\mathfrak{S}_n$ dont l'une des substitutions T est de la forme $T = (b_1 b_2 b_3 b_4 b_5 b_6)$, où $b_1, b_2, b_3, b_4, b_5, b_6$ sont six nombres distincts quelconques de la suite $1, 2, \ldots, n$.

Pour résoudre ce problème, nous examinerons d'abord tous les groupes que peuvent engendrer deux cycles *connexes* du sixième ordre, c'est-à-dire deux cycles du sixième ordre qui ont au moins un élément commun. Nous démontrerons que si un groupe primitif de substitutions G contient deux cycles connexes et imprimitifs indépendants du sixième ordre, alors G est le groupe symétrique des substitutions des éléments permutés. Cette proposition curieuse en soi est très utile pour l'étude que nous avons entreprise. Nous examinerons ensuite les groupes que peut engendrer un système conexe et primitif quelconque de cycles du sixième ordre [1]) et nous en déduirons les critères permettant de discerner toutes les bases du groupe $\mathfrak{S}_n$ dont l'une des substitutions est un cycle du sixième ordre.

---

[1]) Un système de cycles qui permutent un ensemble E d'éléments est dit connexe s'il n'existe aucun sous-ensemble propre E_j de E composé de la totalité des éléments de certains cycles du système envisagé. Un système connexe de cycles est dit primitif s'il est impossible de décomposer l'ensemble E des éléments permutés par les différents cycles du système en une somme de $k \geqslant 2$ sous-ensembles $E_1, \ldots, E_k$, tels que

$$\overline{\overline{E}}_1 = \overline{\overline{E}}_2 = \cdots = \overline{\overline{E}}_k \geqslant 2, \quad E_i E_j = 0 \text{ si } i \neq j, \quad E = E_1 + \cdots + E_k$$

et que, quels que soient les indices i et j $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$ et quel que soit le cycle C du système envisagé, si C transforme au moins un élément de E_i en un élément de E_j, alors C transforme tout l'ensemble E_i en E_j, et le système est dit imprimitif dans le cas contraire. Rappelons que le symbole $\overline{\overline{E}}_i$ désigne la puissance de l'ensemble E_i.

§ 2. Les divers groupes que peuvent engendrer deux cycles connexes du sixième ordre

Soient C_1 et C_2 deux cycles connexes du sixième ordre. Soit n le nombre total des éléments qu'ils permutent et soient $1, 2, \ldots, n$ ces éléments. Soient $C_1 = (1\ 2\ 3\ 4\ 5\ 6)$ et soit h le nombre d'éléments communs à C_1 et à C_2. Comme C_1 et C_2 sont connexes, on a $1 \leq h \leq 6$.

a) *Supposons d'abord que* $h = 6$. Alors $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où $b_1 b_2 b_3 b_4 b_5 b_6$ est une permutation quelconque des nombres 1, 2, 3, 4, 5, 6. Il y a donc en tout 120 cycles C_2 différents.

a_1) *Les deux cycles C_1 et C_2 sont primitifs* (ce qui se produit dans 102 cas). Alors deux éventualités peuvent se présenter.

a_{11}) C_2 est l'un des 18 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 4\ 5\ 3\ 2\ 6)$, $j = \pm 1$, et $i = 1, 2, 3, 4, 5, 6$, ou bien $U = (1\ 3\ 5\ 2\ 6\ 4)$, $j = 1$, $i = 1, 2, 3, 4, 5, 6$, et alors C_1 et C_2 engendrent le groupe G_{120}, d'ordre 120 et de degré 6, trois fois transitif, simplement isomorphe au groupe symétrique $\mathfrak{S}_5$.

Le groupe G_{120} peut être caractérisé par les quatre relations $S^6 = 1$, $T^2 = 1$, $(TS^4)^3 = 1$, $(TS)^4 = 1$. Il se compose de 20 substitutions du type 6*), 20 substitutions du type 3.3, 24 substitutions du type 5, 30 substitutions du type 4, 15 substitutions du type 2.2, 10 substitutions du type 2.2.2 et de la substitution identique. Si l'on répartit les substitutions de G_{120} en classes de substitutions conjuguées, en prenant dans une même classe deux substitutions de G_{120} dans le cas et ce cas seulement où l'une de ces substitutions est la transformée de l'autre par une substitution du groupe G_{120}, on constate que deux substitutions semblables de G_{120} font toujours partie d'une même classe. La condition nécessaire et suffisante pour que deux substitutions de G_{120}, dont l'une au moins est impaire, constituent une base de ce groupe, c'est qu'elles soient connexes et primitives. Le groupe G_{120} possède des bases des douze types[2]) suivants: (6,6), (6,5), (6,4), (6,3.3), (6,2.2.2), (6,2.2), (5,4), (5,2.2.2), (4,4), (4,3.3), (4,2.2.2) et (4,2.2). Il a notamment 180 bases du type (6,6), 360 bases du type (6,3.3), 480 bases du type (6,5), 600 bases du type (6,4), 120 bases du type (6,2.2.2), 240 bases du type (6,2.2), 240 bases du type (5,2.2.2), 480 bases du type (5,4), 120 bases du type (4,2.2.2), 360 bases du type (4,3.3), 120 bases du type (4,2.2) et 120 bases du type (4,4). Le nombre

---

[2]) Soient n, $a_1, a_2, \ldots, a_k$ $(a_1 \geqslant a_2 \geqslant \cdots \geqslant a_k)$ des entiers > 1 et soit S une substitution du groupe $\mathfrak{S}_n$. Nous dirons que la substitution S est du type $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ s'il est possible d'ordonner les cycles d'ordre > 1 de S en une suite $C_1, C_2, \ldots, C_k$, telle que le cycle C_i est d'ordre a_i, $i = 1, 2, \ldots, k$.

Soit G un sous-groupe transitif et primitif de $\mathfrak{S}_n$, à base du second ordre. Nous dirons qu'une base S, T de G est du type (a, b) si la substitution S est du type a et si T est du type b. Une base S, T de G est dite de première espèce et du genre 1 s'il n'existe aucune substitution R de $\mathfrak{S}_n$, telle que $RSR^{-1} = T$, $RTR^{-1} = S$, et elle est dite de première espèce et du genre 2 s'il existe une substitution de l'ensemble $\mathfrak{S}_n - G$ qui transforme S en T et T en S. Une base S, T de G est dite de seconde espèce s'il existe une substitution R de G, telle que $RSR^{-1} = T$ et que $RTR^{-1} = S$.

total de bases de G_{120} est $3420 = 57 \times 60$. C'est un multiple de la moitié de l'ordre du groupe considéré. 3120 bases de G_{120} sont de première espèce et du genre 1 et 300 bases sont de seconde espèce[2]). Notamment, toutes les bases de l'un des types (6,6) ou (4,4) sont de seconde espèce. Le groupe G_{120} est composé. Il admet pour seul vrai sous-groupe distingué le groupe G_{60} d'ordre 60 formé de toutes les substitutions de classe paire de G_{120}. Il n'existe aucune substitution de l'ensemble $\mathfrak{S}_6 - G_{120}$ qui soit permutable avec G_{120}.

a_{12}) C_2 est l'un des 84 cycles du sixième ordre de $\mathfrak{S}_6$, primitifs avec C_1 et qui ne font pas partie de G_{120}. Alors C_1 et C_2 engendrent le groupe symétrique $\mathfrak{S}_6$.

a_2) *Les deux cycles C_1 et C_2 sont imprimitifs.* Il y a au total 18 cycles C_2 imprimitifs avec C_1. Deux cas sont alors à distinguer.

a_{21}) *C_1 et C_2 ont pour systèmes d'imprimitivité les deux ensembles* $\{1,3,5\}$ *et* $\{2,4,6\}$. Ce cas se subdivise en les trois suivants:

a'_{21}) $C_2 = C_1^{\pm 1}$ et alors C_1 et C_2 engendrent le groupe cyclique G_6 d'ordre 6.

a''_{21}) $C_2 = C_1^i U^j C_1^{-i}$, où $U = (1\,2\,5\,6\,3\,4)$, $j = \pm 1$, $i = 1, 2$, et alors C_1 et C_2 engendrent le groupe imprimitif G_{18}, d'ordre 18, qui se compose de six substitutions du type 6, 4 substitutions du type 3.3, 4 substitutions du type 3, 3 substitutions du type 2.2.2 et de la substitution identique. Deux substitutions du type 6 de G_{18}, dont l'une n'est pas une itérée de l'autre, constituent toujours une base de G_{18}.

a'''_{21}) $C_2 = C_1^i U^j C_1^{-i}$, où $U = (1\,2\,3\,6\,5\,4)$, $j = \pm 1$, $i = 1, 2, 3$, et alors C_1 et C_2 engendrent le groupe imprimitif G_{36} d'ordre 36, composé de 12 substitutions du type 6, 4 substitutions du type 3.3, 4 substitutions du type 3, 6 substitutions du type 2.2.2, 9 substitutions du type 2.2 et de la substitution identique. Deux substitutions du type 6 de G_{36}, qui ne font pas toutes deux partie du groupe G_{18}, engendrent toujours le groupe G_{36}. On a $G_{18} \subset G_{36}$.

a_{22}) *C_1 et C_2 ont pour systèmes d'imprimitivité les ensembles* $\{1,4\}$, $\{2,5\}$ *et* $\{3,6\}$, mais non pas $\{1, 3, 5\}$ et $\{2, 4, 6\}$. Alors $C_2 = C_1^i U^j C_1^{-i}$, où $U = (1\,3\,2\,4\,6\,5)$, $j = \pm 1$, $i = 1, 2, 3$, et alors C_1 et C_2 engendrent le groupe imprimitif G_{24}, d'ordre 24, composé de 8 substitutions du type 6, 8 substitutions du type 3.3, 1 substitution du type 2.2.2, 3 substitutions du type 2.2, 3 substitutions du type 2 et de la substitution identique. Deux substitutions du type 6 de G_{24}, dont l'une n'est pas une itérée de l'autre, engendrent toujours le groupe G_{24}.

b) *Supposons maintenant que* $h = 5$. Donc $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où cinq des nombres $b_1, b_2, b_3, b_4, b_5, b_6$ font partie de la suite 1, 2, 3, 4, 5, 6 et le sixième est 7. Il y a 720 cycles C_2, C_1 et C_2 sont alors toujours primitifs. Le cas b) se subdivise en les trois suivants

b_1) C_2 est l'un des 12 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 3\ 4\ 2\ 5\ 7)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors les deux substitutions C_1 et C_2 engendrent le groupe métacyclique ${}_1G_{42}$, d'ordre 42.

Le groupe ${}_1G_{42}$ comprend 6 substitutions du type 7, 14 substitutions du type 6, 14 substitutions du type 3.3, 7 substitutions du type 2.2.2 et la substitution identique. Ce groupe est caractérisé par les trois relations fondamentales $S^6 = 1$, $T^6 = 1$, $T^3 S T^2 S^4 = 1$. Le groupe ${}_1G_{42}$ possède des bases des cinq types (7,6), (6,6), (6,3.3), (6,2.2.2), (3.3,2.2.2). Toute substitution du type 7 forme avec toute substitution du type 6 de ${}_1G_{42}$ une base de ce groupe. La condition nésessaire et suffisante pour qu'une substitution A du type 6 forme une base de ${}_1G_{42}$ avec une substitution B de l'un des types 6, 3.3 ou 2.2.2, c'est que A et B soient connexes. De même, la condition nécessaire et suffisante pour qu'une substitution A du type 3.3 forme avec une substitution B du type 2.2.2 de ${}_1G_{42}$ une base de ce groupe, c'est que A et B soient connexes. Le groupe ${}_1G_{42}$ possède au total 504 $= 12 \times 42$ bases, dont 84 sont du type (7,6), 84 du type (6,6), 168 du type (6,3.3), 84 du type (6,2.2.2) et 84 du type (3.3,2.2.2). 462 bases de ${}_1G_{42}$ sont de première espèce et du genre 1 et 42 sont de seconde espèce. Le nombre total de bases de ${}_1G_{42}$ est un multiple de l'ordre de ce groupe. Aucune substitution de $\mathfrak{S}_7 - {}_1G_{42}$ n'est permutable avec le groupe ${}_1G_{42}$. Le groupe ${}_1G_{42}$ est composé et admet pour vrais sous-groupes distingués le groupe G_{21} composé de toutes les substitutions paires de ${}_1G_{42}$, le groupe G_{14} composé de toutes les substitutions des types 7, 2.2.2 et 1 de ${}_1G_{42}$ ainsi que le groupe cyclique G_7 d'ordre 7 engendré par chaque substitution du type 7 de ${}_1G_{42}$.

b_2) C_2 est l'une des 12 substitutions $C_1^i U^j C_1^{-i}$, où $U = (1\ 4\ 2\ 3\ 5\ 7)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe ${}_2G_{42}$ d'ordre 42, simplement isomorphe avec ${}_1G_{42}$, mais $\neq {}_1G_{42}$, et on a ${}_2G_{42} = R_1 G_{42} R^{-1}$, $R = (2\ 4\ 3)\ (6\ 7)$.

Donc, dans 24 cas, C_1 et C_2 ne constituent pas une base de $\mathfrak{S}_7$.

b_3) $C_2 \overline{\in} {}_1G_{42} + {}_2G_{42}$. 696 cycles C_2 sont dans ce cas et C_1 et C_2 forment alors toujours une base de $\mathfrak{S}_7$.

c) *Supposons maintenant que* $h = 4$. Donc $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où quatre des nombres $b_1, b_2, b_3, b_4, b_5, b_6$ font partie de la suite 1, 2, 3, 4, 5, 6 et les deux autres sont 7 et 8. Il y a en tout 1800 cycles C_2 différents. Ce cas se subdivise en les suivants

c_1) C_2 est l'un des 24 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 2\ 7\ 4\ 5\ 8)$ ou $U = (1\ 5\ 7\ 4\ 2\ 8)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 sont imprimitifs, ils ont pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2,5\}$, $\{3,6\}$, $\{7,8\}$ et ils engendrent le groupe imprimitif G_{192}, d'ordre

192, composé de 32 substitutions du type 6, 32 substitutions du type 3.3, 32 substitutions du type 6.2, 32 substitutions du type 3.3.2, 24 substitutions du type 4.2.2, 12 substitutions du type 4.4, 13 substitutions du type 2.2.2.2, 4 substitutions du type 2.2.2, 6 substitutions du type 2.2, 4 substitutions du type 2 et de la substitution identique.

c_2) Les cycles C_1 et C_2 *sont primitifs*. Trois cas sont alors possibles :

c_{21}) C_2 est l'un des 30 cycles $C_1^i U^j C_1^{-1}$, où U est l'une des substitutions (1 4 3 7 8 2), (1 5 3 8 2 7), $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$, ou encore $U = (1\ 6\ 8\ 3\ 4\ 7)$, $j = 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe trois fois transitif ${}_1G_{336}$, d'ordre 336, et de degré 8.

Le groupe ${}_1G_{336}$ se compose de 84 substitutions du type 8, 48 du type 7, 56 du type 6, 42 du type 4.4, 56 du type 3.3, 21 du type 2.2.2.2, 28 du type 2.2.2 et de la substitution identique. Le groupe G_{336} est formé des substitutions $U^i V^j W^k$, où $U = (3\ 4\ 8\ 7\ 5\ 6)$, $V = (2\ 8\ 3\ 4\ 5\ 7\ 6)$, $W = (1\ 7\ 4\ 6\ 2\ 8\ 5\ 3)$, $i = 1.2.3.4.5.6$, $j = 1, 2, 3, 4, 5, 6, 7$ et $k = 1, 2, 3, 4, 5, 6, 7, 8$. Le groupe ${}_1G_{336}$ peut être caractérisé par les cinq relations fondamentales $S^6 = 1$, $(T^2S^2)^2 = 1$, $(TS)^3 = 1$, $TS^3TS^5T^3S^5 = 1$ et $TS^4T^2S^3T^2S^4 = 1$. Les substitutions de ${}_1G_{336}$ se répartissent en neuf classes de substitutions conjuguées, dont deux comprennent, chacune, 42 substitutions du type 8 et les 7 autres comprennent respectivement toutes les substitutions des types 7, 6, 3.3, 4.4, 2.2.2.2, 2.2.2 et 1 de ${}_1G_{336}$. Le groupe ${}_1G_{336}$ possède au total $34776 = 207 \times 168$ bases. Ce nombre est un multiple de la moitié de l'ordre du groupe considéré. Il y a 3360 bases du type (8,8), 4032 bases du type (8,7), 4704 bases du type (8,6), 4704 bases du type (8,3.3), 3360 bases du type (8,4.4), 1344 bases du type (8,2.2.2.2), 2016 bases du type (8,2.2.2), 2016 bases du type (7,6), 1008 bases du type (7,2.2.2), 840 bases du type (6,6), 1680 bases du type (6,3.3), 2352 bases du type (6,4.4), 1008 bases du type (6,2.2.2.2), 672 bases du type (6,2.2.2), 672 bases du type (3.3,2.2.2), et 1008 bases du type (4.4,2.2.2). Il y a donc des bases de 16 types différents. 32256 bases de ${}_1G_{336}$ sont de première espèce et du genre 1 alors que 2520 bases sont de seconde espèce. Notamment toutes les bases du type 6,6 et la moitié des bases du type 8,8 sont de seconde espèce. Il n'existe aucune substitution de l'ensemble $\mathfrak{S}_8 - {}_1G_{336}$ qui soit permutable avec le groupe ${}_1G_{336}$. Le groupe ${}_1G_{336}$ est un groupe composé. Il admet un vrai sous-groupe distingué G_{168}, d'ordre 168, composé des substitutions de classe paire de ${}_1G_{336}$; le groupe G_{168} est simple et il est simplement isomorphe au groupe intersection de ${}_1G_{1344}$ et ${}_2G_{1344}$ [3]).

c_{22}) C_2 est l'un des 30 cycles $C_1^i U^j C_1^{-i}$, où U est l'une des substitutions (1 4 3 8 7 2), (1 5 3 7 2 8), $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$, ou bien $U = (1\ 6\ 7\ 3\ 4\ 8)$, $j = 1$, $i = 1, 2, 3, 4, 5, 5, 6$, alors C_1 et C_2 engendrent le groupe ${}_2G_{336}$, d'ordre 336, simplement isomorphe à ${}_1G_{336}$ mais $\neq {}_1G_{336}$ et on a ${}_2G_{336} = (7\ 8)\ {}_1G_{336}\ (7\ 8)$.

---

[3]) Voir *S. Piccard*, Les groupes engendrés par un système connexe de cycles d'ordre sept et les bases des groupes symétrique et alterné de degré $n \geqslant 10$ dont l'une des substitutions est un cycle du septième ordre, Comment. Math. Helv., vol. 24, 1950, fasc. 1, p. 6.

c_{23}) Dans les 1716 cas restants où C_1 et C_2 sont primitifs mais où $C_2 \overline{\in} {}_1G_{336} + {}_2G_{336}$, C_1 et C_2 engendrent le groupe symétrique $\mathfrak{S}_8$.

d) *Soit à présent* $h = 3$. Donc $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où trois des nombres $b_1, b_2, b_3, b_4, b_5, b_6$ font partie de la suite 1, 2, 3, 4, 5, 6 et les trois autres sont 7, 8 et 9. Il y a en tout 2400 cycles C_2 différents.

d_1) *Supposons d'abord que C_1 et C_2 sont imprimitifs.* C_1 et C_2 ont alors pour systèmes d'imprimitivité les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$ et $\{7, 8, 9\}$. Il existe 24 cycles C_2 imprimitifs avec C_1. Deux cas sont à distinguer.

d_{11}) C_2 est l'un des 12 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 7\ 3\ 8\ 5\ 9)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors G_1 et G_2 engendrent le groupe imprimitif ${}_1G_{162}$, d'ordre 162 et de degré 9, comprenant 36 substitutions du type 9, 18 substitutions du type 6, 26 substitutions du type 3.3.3, 12 substitutions du type 3.3, 6 substitutions du type 3, 18 substitutions du type 3.2.2.2, 9 substitutions du type 2.2.2, 36 substitutions du type 6.3 et la substitution identique.

d_{12}) C_2 est l'un des 12 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 7\ 3\ 9\ 5\ 8)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe imprimitif ${}_2G_{162}$, d'ordre 162, simplement isomorphe à ${}_1G_{162}$, mais $\neq {}_1G_{162}$, et on a ${}_2G_{162} = (8\ 9)\ {}_1G_{162}\ (8\ 9)$.

d_2) *Supposons maintenant que C_1 et C_2 sont primitifs.* Il existe 2376 cycles C_2 primitifs avec C_1 et chacun de ces cycles ferme avec C_1 une base du groupe symétrique $\mathfrak{S}_9$.

e) *Soit à présent* $h = 2$. Donc $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où deux des nombres $b_1, b_2, b_3, b_4, b_5, b_6$ font partie de la suite 1, 2, 3, 4, 5, 6 et les quatre autres sont 7, 8, 9, 10. Il y a 1800 cycles C_2 différents.

e_1) *Les deux cycles C_1 et C_2 sont imprimitifs.*

72 cycles C_2 sont imprimitifs avec C_1 et trois cas sont à distinguer.

e_{11}) C_2 est l'un des 24 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 7\ 8\ 4\ 9\ 10)$ ou $U = (1\ 9\ 8\ 4\ 7\ 10)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe imprimitif ${}_1G_{1920}$ d'ordre 1920 et de degré 10, dont les systèmes d'imprimitivité sont les ensembles $\{1,4\}$, $\{2,5\}$, $\{3,6\}$, $\{7,9\}$ et $\{8,10\}$. Ce groupe comprend 384 substitutions du type 10, 384 substitutions du type 5.5, 60 substitutions du type 4.4.2, 60 substitutions du type 4.4, 120 substitutions du type 4.2.2.2, 120 substitutions du type 4.2.2, 80 substitutions du type 3.3.2.2, 160 subssitutions du type 3.3.2, 80 substitutions du type 3.3, 80 substitutions du

type 6.2.2, 160 substitutions du type 6.2, 80 substitutions du type 6, 61 substitutions du type 2.2.2.2.2, 65 substitutions du type 2.2.2.2, 10 substitutions du type 2.2.2, 10 substitutions du type 2.2, 5 substitutions du type 2 et de la substitution identique.

e_{12}) C_2 est l'un des 24 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 8\ 7\ 4\ 9\ 10)$ ou $U = (1\ 8\ 10\ 4\ 9\ 7)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe imprimitif ${}_2G_{1920}$, ayant pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{7, 10\}$ et $\{8, 9\}$. Le groupe ${}_1G_{1920}$ est simplement isomorphe à ${}_1G_{1920}$ et on a ${}_2G_{1920} = (7\ 8)\ {}_1G_{1920}\ (7\ 8)$.

e_{13}) C_2 est l'un des 24 cycles $C_1^i U^j C_1^{-i}$, où $U = (1\ 8\ 9\ 4\ 7\ 10)$ ou $U = (1\ 10\ 8\ 4\ 9\ 7)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Alors C_1 et C_2 engendrent le groupe imprimitif ${}_3G_{1920}$, d'ordre 1920, dont les systèmes d'imprimitivité sont les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{7, 8\}$ et $\{9, 10\}$. Le groupe ${}_3G_{1920}$ est simplement isomorphe à ${}_1G_{1920}$ et on a ${}_3G_{1920} = (7\ 9)\ {}_2G_{1920}\ (7\ 9)$.

e_2) *Les deux cycles C_1 et C_2 sont primitifs.* Ils engendrent alors toujours le groupe $\mathfrak{S}_{10}$.

f) *Soit, enfin,* $h = 1$. Alors $C_2 = (b_1 b_2 b_3 b_4 b_5 b_6)$, où un des nombres $b_1, b_2, b_3, b_4, b_5, b_6$ fait partie de la suite $1, 2, 3, 4, 5, 6$ et les cinq autres sont $7, 8, 9, 10, 11$. Il y a en tout 720 cycles C_2 différents. Chacun de ces cycles est primitif avec C_1 et constitue, avec C_1, une base du groupe symétrique $\mathfrak{S}_{11}$.

Remarque 1. Considérons les cycles du sixième ordre des groupes G_{120}, ${}_1G_{42}$, ${}_2G_{42}$, ${}_1G_{336}$, G_{18}, G_{36}, ${}_1G_{162}$, G_{24}, G_{192} et ${}_1G_{1920}$ et passons en revue ceux de ces cycles qui forment avec le cycle $C_1 = (1\ 2\ 3\ 4\ 5\ 6)$ une base de chacun de ces dix groupes.

Le groupe G_{120} contient les cycles suivants du sixième ordre : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $i = 1, 2, 3, 4, 5, 6$ et $U = (1\ 2\ 4\ 3\ 6\ 5)$, $j = \pm 1$, ou bien $U = (1\ 3\ 5\ 2\ 6\ 4)$, $j = 1$. Chacun des cycles $C_1^i U^j C_1^{-i}$ constitue, avec C_1, une base de G_{120}.

Les cycles d'ordre 6 du groupe ${}_1G_{42}$ sont $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $i = 1, 2, 3, 4, 5, 6$, $j = \pm 1$ et $U = (1\ 3\ 2\ 6\ 7\ 4)$. Chacune des substitutions $C_1^i U^j C_1^{-i}$ constitue, avec C_1, une base de ${}_1G_{42}$.

Les cycles d'ordre 6 du groupe ${}_2G_{42}$ sont $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $i = 1, 2, 3, 4, 5, 6$, $U = (1\ 2\ 4\ 7\ 6\ 3)$, $j = \pm 1$. Chacune des substitutions $C_1^i U^j C_1^{-1}$ forme avec C_1 une base de ${}_2G_{42}$.

Les cycles d'ordre 6 de ${}_1G_{336}$ sont : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $i = 1, 2, 3, 4, 5, 6$, U est l'un des 4 cycles $(1\ 2\ 4\ 8\ 6\ 3)$, $(1\ 2\ 5\ 6\ 8\ 7)$, $(1\ 2\ 6\ 3\ 7\ 5)$,

$(1\,5\,3\,8\,2\,7)$, $j = \pm 1$, ou encore $U = (1\,2\,7\,5\,4\,8)$, $j = 1$. Chacun des cycles $C_1^i U^j C_1^{-i}$, où $U = (1\,2\,5\,6\,8\,7)$ ou $U = (1\,5\,3\,8\,2\,7)$, $j = \pm 1$, ou $U = (1\,2\,7\,5\,4\,8)$, $j = 1$, forme avec C_1 une base de ${}_1G_{336}$.

Les cycles d'ordre 6 de G_{18} sont : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $i = 1, 2$, $U = (1\,2\,5\,6\,3\,4)$, $j = \pm 1$. Chacune des substitutions $C_1^i U^j C_1^{-i}$ forme avec C_1 une base de G_{18}.

Les cycles d'ordre 6 du groupe G_{36} sont $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $U = (1\,2\,5\,6\,3\,4)$, $i = 1, 2$, $j = \pm 1$, ou bien $U = (1\,2\,5\,4\,3\,6)$ $i = 1, 2, 3, 4, 5, 6$, $j = 1$. Chacune des substitutions $C_1^i U^j C_1^{-i}$, $U = (1\,2\,5\,4\,3\,6)$, $i = 1, 2, 3, 4, 5, 6$, forme avec C_1 une base de G_{36}.

Les cycles d'ordre 6 de ${}_1G_{162}$ sont : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $U = (1\,2\,5\,6\,3\,4)$, $j = \pm 1$, $i = 1, 2$, ou bien $U = (1\,7\,3\,8\,5\,9)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Chacune des substitutions $C_1^i U^j C_1^{-i}$, où $U = (1\,7\,3\,8\,5\,9)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$, forme avec C_1 une base de ${}_1G_{162}$.

Les cycles d'ordre 6 du groupe G_{24} sont : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $U = (1\,2\,6\,4\,5\,3)$, $j = \pm 1$, $i = 1, 2, 3$. Chacune des substitutions $C_1^i U^j C_1^{-i}$ forme avec C_1 une base du groupe G_{24}.

Les cycles d'ordre 6 de G_{192} sont : $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $j = \pm 1$, $U = (1\,2\,6\,4\,5\,3)$, $i = 1, 2, 3$, ou bien U est l'un des deux cycles $(1\,2\,7\,4\,5\,8)$, $(1\,3\,7\,4\,6\,8)$ et $i = 1, 2, 3, 4, 5, 6$. Chacune des substitutions $C_1^i U C_1^{-i}$, où $U = (1\,2\,7\,4\,5\,8)$ ou $U = (1\,3\,7\,4\,6\,8)$, forme avec C_1 une base de G_{192}.

Les cycles d'ordre 6 de ${}_1G_{1920}$ sont $C_1^{\pm 1}$ et $C_1^i U^j C_1^{-i}$, où $U = (1\,3\,2\,4\,6\,5)$, $j = \pm 1$, $i = 1, 2, 3$, ou bien U est l'un des six cycles $(1\,2\,8\,4\,5\,10)$, $(1\,5\,10\,4\,2\,8)$, $(1\,2\,7\,4\,5\,9)$, $(1\,5\,9\,4\,2\,7)$, $(1\,7\,8\,4\,9\,10)$, $(1\,7\,10\,4\,9\,8)$, $j = \pm 1$, $i = 1, 2, 3, 4, 5, 6$. Chacune des substitutions $C_1^i U^j C_1^{-i}$, où $U = (1\,7\,8\,4\,9\,10)$ ou $U = (1\,7\,10\,4\,9\,8)$, forme avec C_1 une base de ${}_1G_{1920}$.

§ 3. La proposition fondamentale I et sa démonstration

Définition. Soit G un groupe transitif de substitutions et soit C un cycle d'ordre >1. Soit E l'ensemble des éléments permutés par les substitutions de G et soit E' l'ensemble des éléments permutés par C. Nous dirons que *le cycle C et le groupe G sont connexes* si les ensembles E et E' ont au moins un élément communs. Supposons que G et C sont connexes. Alors nous dirons que *G et C sont imprimitifs* si l'on peut décomposer l'ensemble $E + E'$ en une somme de $k \geq 2$ ensembles $E_1, E_2, \ldots, E_k$, tels que $E_i E_j = 0$, $1 \leq i \leq k$, $1 \leq j \leq k$, $i \neq j$, $\overline{\overline{E}}_1 = \overline{\overline{E}}_2 = \cdots = \overline{\overline{E}}_k \geq 2$, $E + E' = E_1 + E_2 + \cdots + E_k$ et

que, quels que soient les indices i et j compris, au sens large, entre 1 et k et quelle que soit la substitution S de l'ensemble $G + C$, si S transforme au moins un élément de E_i en un élément de E_j, S transforme tout l'ensemble E_i en E_j, et nous dirons que *G et C sont primitifs dans le cas contraire.*

Notations. Soit G un groupe et soit S une substitution qui ne fait pas partie de G. Nous désignerons par le symbole (G, S) le groupe engendré par S et les substitutions du groupe G. D'autre part, $S_1, S_2, \ldots, S_k$ étant des substitutions en nombre fini k quelconque, nous désignons par le symbole $(S_1, S_2, \ldots, S_k)$ le groupe engendré par les substitutions $S_1, \ldots, S_k$.

Proposition I. *Si un groupe transitif et primitif de substitutions des éléments $1, 2, \ldots, n$ contient deux cycles connexes et imprimitifs indépendants du sixième ordre, alors ce groupe est le symètrique $\mathfrak{S}_n$ des substitutions des éléments $1, 2, \ldots, n$.*

La démonstration de la proposition I repose sur les lemmes suivants.

Lemme 1. *Quel que soit le cycle $C = (c_1\, c_2\, c_3\, c_4\, c_5\, c_6)$, connexe et primitif avec le groupe G_{18}, le groupe (G_{18}, S) est le symétrique $\mathfrak{S}$ des substitutions des éléments de l'ensemble $\{1, 2, 3, 4, 5, 6\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.*

Démonstration. Le groupe G_{18} est engendré par les deux substitutions $S = (1\,2\,3\,4\,5\,6)$, $T = (1\,2\,5\,6\,3\,4)$ et on a $(G_{18}, C) = (S, T, C)$. Il suffit donc de montrer que $(S, T, C) = \mathfrak{S}$.

Le groupe G_{18} est imprimitif et a pour systèmes d'imprimitivité les deux ensembles $\{1, 3, 5\}$ et $\{2, 4, 6\}$. Comme C est primitif avec G_{18}, on a $C \bar{\in} G_{18}$. Six cas sont à distinguer.

1) $c_1\, c_2\, c_3\, c_4\, c_5\, c_6$ est une permutation des nombres 1, 2, 3, 4, 5, 6. Comme C est primitif avec G_{18}, $\{c_1, c_3, c_5\} \neq \{1, 3, 5\}$ et $\{c_1, c_3, c_5\} \neq \{2, 4, 6\}$.

Ce cas se subdivise en les trois suivants.

Ou bien les deux substitutions S et C sont primitives et $C \in \mathfrak{S}_6 - G_{120}$. Alors les deux substitutions S et C engendrent le groupe $\mathfrak{S}_6$ et on a aussi $(S, T, C) = \mathfrak{S}_6$.

Ou bien S et C sont primitives et $C \in G_{120}$.

Comme, dans ce cas, $T \neq S^{\pm 1}$, d'après la remarque 1, S et C engendrent alors le groupe G_{120}. Ce groupe contient la substitution $U = (1\,2\,4\,3\,6\,5)$ et cette substitution engendre avec T le groupe $\mathfrak{S}_6$.

En effet, on a $TU = (1\ 5\ 2)$ et cette dernière substitution forme avec T une base de $\mathfrak{S}_6$, d'après la proposition 5, pages 20, *Bases, I* [4]).

Ou bien C et S sont imprimitives. Alors $C \in G_{24}$ et engendre avec S le groupe G_{24}, d'après la remarque 1. Or G_{24} contient la substitution $V = (1\ 3\ 2\ 4\ 6\ 5)$ et on a $T^2 V = (3\ 6)$. Or, d'après la proposition 4, page 13, *Bases, I*, la substitution $(3\ 6)$ forme avec T une base de $\mathfrak{S}_6$.

Donc, dans tous les cas, $(S, T, C) = \mathfrak{S}_6$.

2) C permute cinq des nombres 1, 2, 3, 4, 5, 6 et le nombre 7. Dans ce cas C et S sont toujours primitives et engendrent soit le groupe $\mathfrak{S}_7$ (auquel cas le lemme est démontré), soit l'un des deux groupes ${}_1G_{42}$, ${}_2G_{42}$.

Soit $(S, C) = {}_1G_{42}$. Ce groupe contient la substitution $U = (1\,3\,4\,2\,5\,7)$, on a $(T^3 U^2)^3 = (2\ 7)$ et, d'après le corollaire 2, page 13, *Bases, I*, la substitution $(2\ 7)$ engendre avec T le groupe $\mathfrak{S}_7$. Donc $(S, T, C) = \mathfrak{S}_7$.

Et, si $(S, C) = {}_2G_{42}$, ce dernier groupe contient la substitution $V = (1\ 4\ 2\ 3\ 5\ 7)$ et on a $(T^5 V^2)^3 = (3\ 7)$. Or $(3\ 7)$ et T engendrent $\mathfrak{S}_7$, d'après le corollaire 2, page 13, *Bases I*. On a donc $(S, T, C) = \mathfrak{S}_7$.

3) C permute quatre nombres de la suite 1, 2, 3, 4, 5, 6 et les deux nombres 7 et 8. Montrons qu'alors $(S, T, C) = \mathfrak{S}_8$. En effet, si C et S sont primitives, elles engendrent soit le groupe $\mathfrak{S}_8$ (auquel cas notre assertion est démontrée) soit l'un des deux groupes ${}_1G_{336}$, ${}_2G_{336}$.

Si $(S, C) = {}_1G_{336}$, ce dernier groupe contient la substitution $U = (1\ 4\ 3\ 7\ 8\ 2)$, on a $(T^2 U T)^{10} = (6\ 7\ 8)$ et cette substitution engendre avec T le groupe $\mathfrak{S}_8$, d'après le corollaire 2, page 13, *Bases I*. Et si $(S, C) = {}_2G_{336}$ ce groupe contient la substitution $V = (1\,4\,3\,8\,7\,2)$ et on a $(T^2 V T)^5 = (6\ 7\ 8)$, substitution qui engendre avec T le groupe $\mathfrak{S}_8$.

Supposons maintenant que S et C sont imprimitives. Elles ont alors nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ et $\{7, 8\}$, puisque le groupe (S, T, C) est primitif. Alors $(C, S) = G_{192}$, groupe qui contient la substitution $U = (1\,2\,7\,4\,5\,8)$. On a $(TU)^5 = (3\ 6\ 4)$, cette substitution engendre avec T le groupe $\mathfrak{S}_6$ et $(\mathfrak{S}_6, C) = \mathfrak{S}_8$, d'après le lemme II de Hoyer[5]).

---

[4]) Voir *S. Piccard*, Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier, Paris, Vuibert, 1946, ouvrage que nous citons sous l'abréviation *Bases, I*.

[5]) *Lemme II de Hoyer:* Soit G un groupe de substitutions qui permutent les éléments d'un ensemble E_1. Supposons que G contient l'alterné des substitutions des éléments de l'ensemble E_1. Soit C un cycle d'ordre > 1 qui permute les éléments d'un ensemble E_2, tel que $E_1 E_2 \neq 0$, mais que $E_1 \not\subset E_2$. Alors le groupe (G, C) contient l'alterné des substitutions des éléments de l'ensemble $E_1 + E_3$. (Voir *P. Hoyer*, Verallgemeinerung zweier Sätze aus der Theorie der Substitutionengruppen, Math. Ann., Bd. 46, 1895.)

Donc en tous cas $(S, T, C) = \mathfrak{S}_8$.

4) C permute trois nombres de la suite 1, 2, 3, 4, 5, 6 et les trois nombres 7, 8, 9. Alors, comme le groupe (S, T, C) est primitif, puisque C est primitif avec G_{18}, S et C sont forcément primitives et engendrent le groupe $\mathfrak{S}_9$. Donc $(S, T, C) = \mathfrak{S}_9$.

5) C permute deux des nombres 1, 2, 3, 4, 5, 6 et les quatre nombres 7, 8, 9, 10. Alors, si S et C sont primitives, elles engendrent, d'après ce qui précède, le groupe $\mathfrak{S}_{10}$ et $(S, T, C) = \mathfrak{S}_{10}$. Et, si S et C sont imprimitives, elles ont alors nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ ainsi que $\{7, 9\}$ et $\{8, 10\}$ ou $\{7, 10\}$ et $\{8, 9\}$ ou enfin $\{7, 8\}$ et $\{9, 10\}$ et alors S et C engendrent respectivement le groupe ${}_1G_{1920}$ ou ${}_2G_{1920}$ ou enfin ${}_3G_{1920}$. Si $(S, C) = {}_1G_{1920}$, ce groupe contient la substitution $U = (1\ 7\ 8\ 4\ 9\ 10)$, $(TU)^7 = (1\ 7\ 8)$. La substitution $(1\ 7\ 8)$ engendre, avec S, le groupe $\mathfrak{S}_8$, d'après le corollaire 2, page 13, *Bases I*, et C engendre avec $\mathfrak{S}_8$ le groupe $\mathfrak{S}_{10}$, d'après le lemme II de Hoyer[5]). Donc $(S, T, C) = \mathfrak{S}_{10}$. Si $(S, C) = {}_2G_{1920}$, ce groupe contient la substitution $V = (1\,8\,7\,4\,9\,10)$, $(TV)^7 = (1\ 8\ 7)$, la substitution $(1\ 8\ 7)$ engendre avec S le groupe $\mathfrak{S}_8$ et C engendre avec $\mathfrak{S}_8$ le groupe $\mathfrak{S}_{10}$. Donc $(S, T, C) = \mathfrak{S}_{10}$.

Et, si $(S, C) = {}_3G_{1920}$, ce groupe contient la substitution

$W = (1\ 8\ 9\ 4\ 7\ 10)$, on a $(TW)^7 = (1\ 8\ 9)$, les substitutions $(1\ 8\ 9)$

et S engendrent le groupe symétrique $\mathfrak{S}$ des substitutions des éléments 1, 2, 3, 4, 5, 6, 8, 9 et C engendre avec $\mathfrak{S}$ le groupe $\mathfrak{S}_{10}$. Donc $(S, T, C) = \mathfrak{S}_{10}$.

6) C permute un seul des nombres 1, 2, 3, 4, 5, 6 et les cinq nombres 7, 8, 9, 10, 11. Alors S et C engendrent toujours le groupe $\mathfrak{S}_{11}$, d'après le corollaire 2, page 13, *Bases I*, donc aussi $(S, T, C) = \mathfrak{S}_{11}$.

Le lemme 1 est donc démontré.

Corollaire 1. Quel que soit le cycle C du sixième ordre, connexe et primitif avec le groupe G_{36}, le groupe (G_{36}, C) est le symétrique $\mathfrak{S}$ des substitutions de tous les éléments permutés par C et les substitutions de G_{36}.

Démonstration. Comme G_{18} est un sous-groupe de G_{36}, on a †) $(G_{18}, C) \subset (G_{36}, C)$. Et comme les substitutions des deux groupes (G_{18}, C) et (G_{36}, C) permutent les mêmes éléments, on a, d'après le lemme 1, $(G_{18}, C) = \mathfrak{S}$. Et comme $(G_{36}, C) \subset \mathfrak{S}$, on a, d'après †), $(G_{36}, C) = \mathfrak{S}$, c. q. f. d.

Lemme 2. Quel que soit le cycle du sixième ordre $C = (c_1\, c_2\, c_3\, c_4\, c_5\, c_6)$, *connexe et primitif avec le groupe* G_{24}, *le groupe* (G_{24}, C) *est le symétrique* $\mathfrak{S}$ *des substitutions des éléments de l'ensemble* $\{1, 2, 3, 4, 5, 6\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

Démonstration. On a $G_{24} = (S, T)$, où $S = (1\ 2\ 3\ 4\ 5\ 6)$ et $T = (1\ 3\ 2\ 4\ 6\ 5)$, donc $(G_{24}, C) = (S, T, C)$ et il suffit de démontrer que $(S, T, C) = \mathfrak{S}$. Le groupe G_{24} est imprimitif et admet pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$.

Six cas sont à distinguer.

1) $\{c_1, c_2, c_3, c_4, c_5, c_6\} = \{1, 2, 3, 4, 5, 6\}$.

Alors, si les deux substitutions S et C sont primitives, elles engendrent soit le groupe $\mathfrak{S}_6$, et alors le lemme 2 est démontré dans le cas considéré, soit le groupe G_{120}. Supposons que $(S, C) = G_{120}$. Ce groupe contient la substitution $U = (1\ 2\ 4\ 3\ 6\ 5)$, $(T^4U)^3 = (2\ 3)$ et la substitution $(2\ 3)$ engendre avec S le groupe $\mathfrak{S}_6$ d'après la proposition 1, page 11, *Bases I*. Donc $(S, T, C) = \mathfrak{S}_6$.

Supposons maintenant que S et C sont imprimitives. Comme le groupe (G_{24}, C) est primitif, les substitutions S et C ont alors nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 3, 5\}$ et $\{2, 4, 6\}$. Alors S et C engendrent l'un des deux groupes G_{18} ou G_{36}, groupes qui tous deux contiennent la substitution $U = (1\ 2\ 5\ 6\ 3\ 4)$. Or $T^3U = (1\ 5\ 3)$ et cette substitution engendre avec T le groupe $\mathfrak{S}_6$, d'après la proposition 5, page 20, *Bases I*. Donc $(S, T, C) = \mathfrak{S}_6$.

2) C permute cinq des nombres $1, 2, 3, 4, 5, 6$ et le nombre 7. Alors C et S sont toujours primitives et engendrent soit le groupe $\mathfrak{S}_7$, auquel cas le lemme est démontré, soit l'un des deux groupes ${}_1G_{42}$ ou ${}_2G_{42}$. Si $(S, C) = {}_1G_{42}$, ce groupe contient la substitution $U = (1\ 3\ 4\ 2\ 5\ 7)$, $(T^2U)^4 = (1\ 4\ 6)$, la substitution $(1\ 4\ 6)$ engendre avec S le groupe $\mathfrak{S}_6$, d'après la proposition 5, page 20, *Bases I*, et C engendre avec $\mathfrak{S}_6$, le groupe $\mathfrak{S}_7$, d'après le lemme II de Hoyer. Donc $(S, T, C) = \mathfrak{S}_7$. Et si $(S, C) = {}_2G_{42}$, ce groupe contient la substitution $V = (1\ 2\ 4\ 7\ 6\ 3)$ et on a $(T^2V)^4 = (2\ 5\ 3)$. Or la substitution $(2\ 5\ 3)$ engendre avec S le groupe $\mathfrak{S}_6$ et C engendre avec $\mathfrak{S}_6$ le groupe $\mathfrak{S}_7$. Donc $(S, T, C) = \mathfrak{S}_7$.

3) C permute quatre des nombres $1, 2, 3, 4, 5, 6$ et les deux nombres 7 et 8. S et C sont alors forcément primitives, car le groupe (S, T, C) est primitif et que S et T sont imprimitives et ont pour systèmes d'imprimitivité $\{1, 4\}$, $\{2, 5\}$ et $\{3, 6\}$. Si donc S et C étaient imprimitives, elles devraient avoir pour systèmes d'imprimitivité des ensembles com-

prenant chacun trois éléments, ce qui est impossible puisque S et C permutent au total 8 éléments et que $8 \not\equiv 0 \pmod 3$. Donc S et C engendrent soit le groupe $\mathfrak{S}_8$, auquel cas le lemme est démontré, soit l'un des deux groupes ${}_1G_{336}$, ${}_2G_{336}$. Si $(S, C) = {}_1G_{336}$, ce groupe contient la substitution $U = (1\,4\,3\,7\,8\,2)$ et on a $(TU)^5 = (1\,5\,6)$. Or $(1\,5\,6)$ engendre avec S le groupe $\mathfrak{S}_6$, d'après la proposition 5, page 20, *Bases I*, et C engendre avec $\mathfrak{S}_6$ le groupe $\mathfrak{S}_8$ d'après le lemme II de Hoyer. Donc $(S, T, C) = \mathfrak{S}_8$. Le raisonnement est tout à fait analogue si $(S, C) = {}_2G_{336}$, groupe qui contient la substitution $(1\,4\,3\,8\,7\,2)$.

4) C permute trois des nombres 1, 2, 3, 4, 5, 6 ainsi que les trois nombres 7, 8, 9. Alors si S et C sont primitives, elles engendrent, d'après ce qui précède, le groupe $\mathfrak{S}_9$ et on a aussi $(S, T, C) = \mathfrak{S}_9$. Et si C et S sont imprimitives, elles ont nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$ et $\{7, 8, 9\}$ et engendrent l'un des deux groupes ${}_1G_{162}$ ou ${}_2G_{162}$. Si $(S, C) = {}_1G_{162}$, ce groupe contient la substitution $U = (1\,7\,3\,8\,5\,9)$, $(T^2U)^7 = (3\,8)$, la substitution $(3\,8)$ engendre avec S, d'après le corollaire 2, page 13, *Bases I*, le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, 8 et ce dernier groupe engendre avec C le groupe $\mathfrak{S}_9$, d'après le lemme II de Hoyer. Donc $(S, T, C) = \mathfrak{S}_9$. Le raisonnement est tout à fait analogue si $(S, C) = {}_2G_{162}$.

5) C permute deux des nombres 1, 2, 3, 4, 5, 6 et les quatre nombres 7, 8, 9, 10. Alors, comme le groupe (S, T, C) est primitif, S et C sont nécessairement primitives. En effet, si S et C étaient imprimitives, leurs systèmes d'imprimitivité devraient comprendre chacun trois éléments, ce qui est impossible, puisque S et T permutent, ensemble, 10 éléments et que $10 \not\equiv 0 \pmod 3$. Donc $(S, C) = \mathfrak{S}_{10} = (S, T, C)$.

6) C permute un seul des nombres 1, 2, 3, 4, 5, 6 et les cinq nombres 7, 8, 9, 10, 11. Alors $(S, C) = \mathfrak{S}_{11}$, d'après le corollaire 2, page 13, *Bases I*. Donc aussi $(S, T, C) = \mathfrak{S}_{11}$ et le lemme 2 est démontré.

Lemme 3. Quel que soit le cycle du sixième ordre $C = (c_1\,c_2\,c_3\,c_4\,c_5\,c_6)$, *connexe et primitif avec le groupe* G_{192}, *en composant* C *avec les substitutions de* G_{192} *on obtient le groupe symétrique* $\mathfrak{S}$ *des substitutions des éléments de l'ensemble* $\{1, 2, 3, 4, 5, 6, 7, 8\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

Démonstration. On a $G_{192} = (S, T)$, où $S = (1\,2\,3\,4\,5\,6)$, $T = (1\,2\,7\,4\,5\,8)$ et, comme $(S, T, C) = (G_{192}, C)$, il suffira de montrer que $(S, T, C) = \mathfrak{S}$. Le groupe G_{192} est imprimitif et a pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{7, 8\}$.

Comme la substitution C est connexe et primitive avec le groupe G_{192}, le groupe (S, T, C) est transitif et primitif. Et comme il est de degré ≥ 8, et qu'il contient des substitutions de classe impaire, pour démontrer que $(S, T, C) = \mathfrak{S}$, il suffit de montrer que le groupe (S, T, C) contient un cycle quelconque du second ou du troisième ordre ou encore de montrer que deux quelconques des substitutions S, T, C engendrent le groupe symétrique des substitutions des éléments qu'elles permutent, d'ou il résulte aussitôt, d'après le lemme II de Hoyer, que $(S, T, C) = \mathfrak{S}$.

Sept cas sont à distinguer.

1) C permute les six nombres 1, 2, 3, 4, 5, 6.

Si S et C sont primitives, deux cas sont à distinguer. Ou bien $(S, C) = \mathfrak{S}_6$ et alors T et $\mathfrak{S}_6$ engendrent le groupe $\mathfrak{S}_8$, d'après le lemme II de Hoyer, et alors $(S, T, C) = \mathfrak{S}_8$. Ou bien $(S, C) = G_{120}$, groupe qui contient la substitution $U = (1\ 2\ 4\ 3\ 6\ 5)$, $(T^5U)^2 = (3\ 4\ 6)$ et cette substitution engendre avec T le groupe $\mathfrak{S}_8$, d'après le corollaire 2, p. 13, *Bases I*. Il s'ensuit que $(S, T, C) = \mathfrak{S}_8$.

Supposons maintenant que S et C sont imprimitives. Alors comme C est primitive avec G_{192}, S et C ont forcément pour systèmes d'imprimitivité les ensembles $\{1, 3, 5\}$ et $\{2, 4, 6\}$ et, par conséquent, (S, C) contient en tout cas le groupe G_{18}. ((S, C) est alors l'un des deux groupes G_{18} ou G_{36}.) Donc le groupe (S, C) contient la substitution $U = (1\ 2\ 5\ 6\ 3\ 4)$. Or $(TU)^{10} = (3\ 5\ 6)$ et cette dernière substitution engendre avec T le groupe $\mathfrak{S}_8$, d'après le corollaire 2, page 13, *Bases I*. Donc $(S, T, C) = \mathfrak{S}_8$.

2) C permute cinq des nombres 1, 2, 3, 4, 5, 6 et un nombre c de l'ensemble $\{7, 8, 9\}$. Les substitutions S et C sont alors primitives et les cas suivants sont alors possibles.

Ou bien S et C engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d'où il résulte que $(S, T, C) = \mathfrak{S}$.

Ou bien S et C engendrent un groupe simplement isomorphe à ${}_1G_{42}$, groupe qui contient soit la substitution $U = (1\ 3\ 2\ 6\ c\ 4)$ soit la substitution $V = (1\ 2\ 4\ c\ 6\ 3)$. Si $c = 7$, on a $(TU)^5 = (2\ 4\ 6)$ et $(T^2V)^3 = (2\ 8)$. Si $c = 8$, on a $(T^2U)^5 = (2\ 6)$, $(TV)^5 = (1\ 4\ 7)$. Et si $c = 9$, on a $(T^5U)^4 = (4\ 8\ 5)$ et $(T^2V)^7 = (2\ 8)$. Donc dans tous les cas $(S, T, C) = \mathfrak{S}$.

3) C permute quatre des nombres 1, 2, 3, 4, 5, 6 et les deux nombres c, d $(c < d)$ qui forment l'un des couples $\{7, 8\}$, $\{7, 9\}$, $\{8, 9\}$, $\{9, 10\}$. Dans ce cas encore S et C sont forcément primitives, car elles permutent

ensemble huit éléments et que, comme le groupe (S, T, C) est primitif, si S et C étaient imprimitives, leurs systèmes d'imprimitivité devraient comprendre trois éléments chacun, ce qui est impossible puisque $8 \not\equiv 0 \pmod 3$. Deux cas peuvent se présenter. Ou bien S et C engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d et, par suite, $(S, T, C) = \mathfrak{S}$. Ou bien le groupe (S, C) est simplement isomorphe à ${}_1G_{336}$ et comprend l'une des deux substitutions $U = (1\,4\,3\,c\,d\,2)$, $V = (1\,4\,3\,d\,c\,2)$. Alors, si $c = 7$ et $d = 8$, on a $(T^2U)^5 = (2\,7)$ et $(T^2V)^4 = (1\,8\,5)$. Si $c = 7$ et $d = 9$, on a $(TU)^4 = (1\,5\,8)$, $(T^2V^2)^4 = (1\,3\,5)$. Si $c = 8$ et $d = 9$, on a $(T^5U)^5 = (3\,4\,5)$ et $(T^4V)^8 = (3\,4\,9)$. Si $c = 9$ et $d = 10$, on a $(TU)^{10} = (1\,5\,8)$, $(TV)^{10} = (1\,5\,8)$. Donc dans tous les cas $(S, T, C) = \mathfrak{S}$.

4) C permute trois des nombres 1, 2, 3, 4, 5, 6 ainsi que trois nombres c, d, e $(c<d<e)$ qui forment l'un des cinq ensembles $\{7, 8, 9\}$, $\{7, 8, 10\}$, $\{7, 9, 10\}$, $\{8, 9, 10\}$ ou $\{9, 10, 11\}$. Si les substitutions S et C sont primitives, elles engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d, e et $(S, T, C) = \mathfrak{S}$. Supposons maintenant que S et C sont imprimitives. Comme le groupe (S, T, C) est primitif, S et C ont alors nécessairement pour systèmes d'imprimitivité les trois ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, $\{c, d, e\}$ et l'un des deux ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$ comprend les trois éléments de la suite 1, 2, 3, 4, 5, 6 qui sont permutés par C.

Les substitutions S et C engendrent alors un groupe simplement isomorphe à ${}_1G_{162}$, groupe qui contient l'une des deux substitutions $U = (1\,c\,3\,d\,5\,e)$ ou $V = (1\,c\,3\,e\,5\,d)$. Si $c = 7$, $d = 8$ et $e = 9$, on a $(T^3U^2)^5 = (8\,9)$ et $(TV)^{10} = (1\,4\,5)$. Si $c = 7$, $d = 8$ et $e = 10$, on a $(T^4U)^5 = (5\,10)$, $(TV)^{10} = (1\,4\,5)$. Si $c = 7$, $d = 9$ et $e = 10$, on a $(T^4U)^3 = (5\,10)$, $(T^4V)^3 = (5\,9)$. Si $c = 8$, $d = 9$ et $e = 10$, on a $(TU)^5 = (3\,8\,9)$, $(TV)^5 = (3\,8\,10)$. Enfin, si $c = 9$, $d = 10$ et $e = 11$, les cycles C et T ont alors en commun soit les deux nombres 1, 5, soit les deux nombres 2, 4 et ils sont primitifs. En effet, comme le groupe (S, T, C) est primitif, si les deux substitutions T et C étaient imprimitives, leurs systèmes d'imprimitivité devraient contenir trois éléments chacun, ce qui est impossible puisque l'un de ces systèmes doit être composé des éléments communs aux deux cycles T et C. Donc les deux substitutions T et C engendrent le groupe symétrique des substitutions des éléments 1, 2, 4, 5, 7, 8, 9, 10, 11 et, par conséquent, $(S, T, C) = \mathfrak{S}$.

5) C permute deux des nombres 1, 2, 3, 4, 5, 6 et quatre nombres

c, d, e, f supérieurs à 6. S et C sont alors nécessairement primitives et engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc $(S, T, C) = \mathfrak{S}$.

6) C permute un seul des nombres, 1, 2, 3, 4, 5, 6, ainsi que cinq nombres c, d, e, f, g supérieurs à 6. Alors S et C engendrent le symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d, e, f, g et on a $(S, T, C) = \mathfrak{S}$.

7) C ne permute aucun des nombres 1, 2, 3, 4, 5, 6. Comme C est connexe avec le groupe ${}_1G_{192}$, C permute alors l'un au moins des deux nombres 7, 8.

Supposons d'abord que C permute les deux nombres 7 et 8, ainsi que les nombres 9, 10, 11, 12. Les substitutions T et C sont forcément primitives. En effet, comme le groupe (S, T, C) est primitif, si T et C étaient imprimitives, les ensembles $\{1, 7, 5\}$ et $\{3, 4, 8\}$ devraient alors constituer deux systèmes d'imprimitivité de C et T, ce qui est impossible, d'après les hypothèses faites sur C. Donc T et C sont bien primitives et engendrent le groupe symétrique des substitutions des éléments 1, 2, 4, 5, 7, 8, 9, 10, 11, 12. Il s'ensuit que $(S, T, C) = \mathfrak{S}$.

Supposons enfin que C permute l'un des deux nombres 7, 8 ainsi que les cinq nombres 9, 10, 11, 12, 13. Alors T et C engendrent le symétrique des substitutions des éléments 1, 2, 4, 5, 7, 8, 9, 10, 11, 12, 13 et $(S, T, C) = \mathfrak{S}$.

Le lemme 3 est donc démontré.

Lemme 4. Quel que soit le cycle du sixième ordre $C = (c_1 c_2 c_3 c_4 c_5 c_6)$ *connexe et primitif avec le groupe* ${}_1G_{162}$, *en composant* C *avec les substitutions du groupe* ${}_1G_{162}$ *on obtient le groupe symétrique* $\mathfrak{S}$ *des substitutions des éléments de l'ensemble* $\{1, 2, 3, 4, 5, 6, 7, 8, 9\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

Démonstration. Le groupe ${}_1G_{162}$ est imprimitif et admet pour systèmes d'imprimitivité les trois ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, $\{7, 8, 9\}$. On a ${}_1G_{162} = (S, T)$, où $S = (1\ 2\ 3\ 4\ 5\ 6)$ et $T = (1\ 7\ 3\ 8\ 5\ 9)$. Donc $({}_1G_{162}, C) = (S, T, C)$ et pour démontrer le lemme 4, il suffit de prouver que $(S, T, C) = \mathfrak{S}$. Comme C est connexe et primitif avec ${}_1G_{162}$, le groupe (S, T, C) est transitif et primitif. Donc pour démontrer que $(S, T, C) = \mathfrak{S}$, il suffit de prouver que le groupe (S, T, C) contient un cycle quelconque du second ou du troisième ordre ou encore de prouver que deux quelconques des substitutions S, T, C engendrent le groupe symétrique des substitutions des éléments qu'elles permutent.

Sept cas sont à distinguer.

1) C permute les six nombres 1, 2, 3, 4, 5, 6. Si S et C sont primitives, ou bien elles engendrent le groupe $\mathfrak{S}_6$ et alors $(S, T, C) = \mathfrak{S}_9$, ou bien $(S, C) = G_{120}$, groupe qui contient la substitution $U = (1\,2\,4\,3\,6\,5)$ et on a $(T^4U)^3 = (3\,6)$, donc $(S, T, C) = \mathfrak{S}_9$. Et si S et C sont imprimitives, elles ont alors nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$ et $\{3, 6\}$ et $(S, C) = G_{24}$, groupe qui contient la substitution $U = (1\,3\,2\,4\,6\,5)$ et on a $(TU^2)^7 = (5\,8)$. Donc $(S, T, C) = \mathfrak{S}_9$.

2) C permute cinq des nombres 1, 2, 3, 4, 5, 6 et un nombre c de l'ensemble $\{7, 8, 9, 10\}$. S et C sont alors toujours primitives et engendrent soit le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, ce qui implique que $(S, T, C) = \mathfrak{S}$, soit un groupe simplement isomorphe au groupe ${}_1G_{42}$, qui contient l'une des deux substitutions $U = (1\,3\,2\,6\,c\,4)$, $V = (1\,2\,4\,c\,6\,3)$. Si $c = 7$, on a $(TU)^4 = (2\,6\,3)$, $(T^4V)^7 = (3\,5)$. Si $c = 8$, on a $(T^2U)^7 = (1\,5)$ et $(T^3V)^4 = (1\,2\,4)$. Si $c = 9$, on a $(T^2U)^7 = (1\,5)$ et $(TV)^4 = (1\,2\,4)$. Et, si $c = 10$, on a $(T^2U)^{15} = (1\,5)$ et $(T^4V)^{15} = (3\,5)$. Donc, dans tous les cas, $(S, T, C) = \mathfrak{S}$.

3) C permute quatre des nombres 1, 2, 3, 4, 5, 6 ainsi que les deux nombres c et d $(c<d)$ qui forment l'un des couples $\{7, 8\}$, $\{7, 9\}$, $\{8, 9\}$, $\{7, 10\}$, $\{8, 10\}$, $\{9, 10\}$ ou $\{10, 11\}$. Alors si C et S sont primitives, ou bien elles engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d et $(S, T, C) = \mathfrak{S}$; ou bien le groupe (S, C) est simplement isomorphe à ${}_1G_{336}$ et contient l'une des substitutions $U = (1\,4\,3\,c\,d\,2)$, $V = (1\,4\,3\,d\,c\,2)$. Alors, si $c = 7$ et $d = 8$, on a $(T^2U)^3 = (7\,9)$, $(T^2V)^4 = (1\,4\,5)$; si $c = 7$ et $d = 9$, on a $(T^2U)^4 = (1\,4\,5)$, $(T^2V)^3 = (8\,9)$; si $c = 8$ et $d = 9$, on a $(TU)^{10} = (1\,4\,8)$, $(T^2V)^4 = (1\,4\,5)$; si $c = 7$, $d = 10$, on a $(TU)^{10} = (2\,7\,10)$, $(T^4V)^7 = (1\,4)$; si $c = 8$ et $d = 10$, on a $(T^3U)^4 = (2\,8\,10)$, $(T^4V)^7 = (1\,4)$; si $c = 9$ et $d = 10$, on a $(T^4U)^7 = (1\,4)$, $(T^4V)^7 = (1\,4)$; enfin si $c = 10$ et $d = 11$, on a $(T^4U)^{10} = (7\,9\,8)$ et $(T^4V)^{10} = (7\,9\,8)$. Et si les substitutions S et C sont imprimitives, comme le groupe (S, T, C) est primitif, elles ont alors nécessairement pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ et $\{c, d\}$ et elles engendrent un groupe simplement isomorphe à G_{192}, groupe qui contient la substitution $U = (1\,2\,c\,4\,5\,d)$. Alors si $c = 7$ et $d = 8$, on a $(T^3U)^4 = (1\,2\,5)$; si $c = 7$ et $d = 9$, on a $(TU)^5 = (4\,7\,9)$; si $c = 8$ et $d = 9$, on a $(TU)^{10} = (1\,2\,5)$; si $c = 7$ et $d = 10$, on a

$(T^4U)^7 = (5\ 10)$; si $c = 8$ et $d = 10$, on a $(T^4U)^7 = (5\ 10)$; si $c = 9$ et $d = 10$, on a $(T^4U)^7 = (5\ 10)$: enfin, si $c = 10$ et $d = 11$, on a $(T^4U)^{10} = (7\ 9\ 8)$. Donc, dans tous ces cas $(S, T, C) = \mathfrak{S}$.

4) C permute trois des nombres 1, 2, 3, 4, 5, 6 et trois nombres c, d, e supérieurs à 6. Alors, comme le groupe (S, T, C) est primitif, les substitutions S et C sont nécessairement primitives et engendrent le groupe symétrique des substitutions des éléments $1, 2, 3, 4, 5, 6, c, d, e$. Donc $(S, T, C) = \mathfrak{S}$.

5) C permute deux des nombres 1, 2, 3, 4, 5, 6 et quatre nombres c, d, e, f supérieurs à 6. Alors, si S et C sont primitives, elles engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d, e, f et $(S, T, C) = \mathfrak{S}$. Et si S et C sont imprimitives, leurs systèmes d'imprimitivité sont alors nécessairement les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ et $\{c, d\}$, $\{e, f\}$ ou $\{c, e\}$, $\{d\ f\}$ ou encore $\{c, f\}$, $\{e, d\}$. Dans ce cas, S et C engendrent un groupe simplement isomorphe à ${}_1G_{1920}$, groupe qui contient une des trois substitutions $U = (1cd4ef)$, $V = (1\ d\ c\ 4\ e\ f)$, $W = (1\ d\ e\ 4\ c\ f)$. Alors si $c = 7$, $d = 8$, $e = 9$ et $f = 10$, on a $(T^5U)^4 = (4\ 5\ 8)$, $(T^2V)^5 = (4\ 7)$, $(T^4W)^5 = (4\ 9)$. D'autre part, si deux des nombres c, d, e, f et deux seulement font partie de l'ensemble $\{7, 8, 9\}$, les cycles C et T ont alors trois éléments communs (savoir un des nombres 1, 3, 5 et deux des nombres 7, 8, 9), ils sont nécessairement primitifs, puisque le groupe (S, T, C) est primitif, et ils engendrent le groupe symétrique des substitutions des éléments qu'ils permutent. Donc $(S, T, C) = \mathfrak{S}$. Supposons maintenant qu'un seul des nombres c, d, e, f, notamment c, fait partie de l'ensemble $\{7, 8, 9\}$. Alors chacune des substitutions U, V, W a avec T deux éléments communs, notamment 1 et c, elle est donc primitive avec T et engendre avec T le symétrique des substitutions des éléments permutés. Donc $(S, T, C) = \mathfrak{S}$.

6) C permute un seul nombre de la suite $1, 2, 3, 4, 5, 6$ et cinq nombres c, d, e, f, g supérieurs à 6. Alors S et C engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d, e, f, g et $(S, T, C) = \mathfrak{S}$.

7) C ne permute aucun des nombres 1, 2, 3, 4, 5, 6. Comme C est connexe avec le groupe ${}_1G_{162}$, C permute alors l'un au moins des nombres 7, 8, 9.

Si C permute les six nombres 7, 8, 9, 10, 11, 12, comme le groupe (S, T, C) est primitif, T et C sont alors forcément primitives. En effet T et C permutent ensemble neuf éléments et si C et T étaient imprimitives, leurs systèmes d'imprimitivité devraient comprendre deux élé-

ments chacun, ce qui est impossible puisque $9 \not\equiv 0 \pmod 2$. Donc T et C sont bien primitives et engendrent, par conséquent, le groupe symétrique des substitutions des éléments 1, 3, 5, 7, 8, 9, 10, 11, 12. Donc $(S, T, C) = \mathfrak{S}$.

Supposons maintenant que C permute deux des nombres 7, 8, 9 et les quatre nombres 10, 11, 12, 13. Dans ce cas aussi, comme le groupe (S, T, C) est primitif, les deux substitutions T et C sont nécessairement primitives, car si T et C étaient imprimitives, elles devraient avoir pour systèmes d'imprimitivité les ensembles $\{1, 8\}$, $\{5, 7\}$, $\{3, 9\}$, ce qui est impossible d'après les hypothèses faites sur C. Donc T et C engendrent le groupe symétrique des substitutions des éléments 1, 3, 5, 7, 8, 9, 10, 11, 12, 13 et, par suite, $(S, T, C) = \mathfrak{S}_{13}$.

Supposons enfin que C permute un seul des nombres 7, 8, 9 et les cinq nombres 10, 11, 12, 13, 14. Alors T et C engendrent le groupe symétrique des substitutions des éléments 1, 3, 5, 7, 8, 9, 10, 11, 12, 13, 14 et $(S, T, C) = \mathfrak{S}_{14}$.

Le lemme 4 est donc démontré.

Corollaire 2. Quel que soit le cycle du sixième ordre C connexe et primitif avec le groupe ${}_2G_{162}$, en composant C avec les substitutions de ${}_2G_{162}$, on obtient le groupe symètrique des substitutions de tous les éléments permutés par C et les substitutions de ${}_2G_{162}$.

Démonstration. Soit C un cycle du sixième ordre connexe et primitif avec ${}_2G_{162}$ et soit $R = (7\ 8)$. On a $R\,{}_2G_{162}R^{-1} = {}_1G_{162}$. Posons $RCR^{-1} = C'$. Comme C et ${}_2G_{162}$ sont connexes et primitifs, il en est de même de C' et de ${}_1G_{162}$. Or, d'après le lemme 4, C' et ${}_1G_{162}$ engendrent le groupe symétrique des substitutions des éléments permutés par C' et les substitutions de ${}_1G_{162}$. Soit $G = ({}_2G_{162}, C)$ et soit $G' = ({}_1G_{162}, C')$. On a $RGR^{-1} = G'$. Donc G et G' sont simplement isomorphes et, comme ces deux groupes sont du même degré, il s'ensuit que G aussi est le symétrique des substitutions des éléments permutés par C et les substitutions de ${}_2G_{162}$. Le corollaire 2 est donc démontré.

Lemme 5. Quel que soit le cycle du sixième ordre $C = (c_1c_2c_3c_4c_5c_6)$ connexe et primitif avec le groupe ${}_1G_{1920}$, en composant C avec les substitutions du groupe ${}_1G_{1920}$, on obtient le groupe symètrique $\mathfrak{S}$ des substitutions des éléments de l'ensemble $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

Démonstration. Le groupe ${}_1G_{1920}$ est imprimitif et a pour systèmes d'imprimitivité les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{7, 9\}$ et $\{8, 10\}$.

On a ${}_1G_{1920} = (S, T)$, ou $S = (1\ 2\ 3\ 4\ 5\ 6)$ et $T = (1\ 7\ 8\ 4\ 9\ 10)$, donc $({}_1G_{1920}, C) = (S, T, C)$ et, par suite, pour démontrer le lemme 5, il suffit de montrer que $(S, T, C) = \mathfrak{S}$.

Comme C est connexe avec ${}_1G_{1920}$, C a au moins un élément commun avec l'un au moins des cycles S, T. Supposons d'abord que C a des éléments communs seulement avec S. Ces éléments communs font alors partie de l'ensemble $\{2, 3, 5, 6\}$. S et C sont alors primitives. En effet, si elles étaient imprimitives, comme le groupe (S, T, C) est primitif, alors que le groupe (S, T) est imprimitif et a pour systèmes d'imprimitivité $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{7, 9\}$ et $\{8, 10\}$, S et C devraient avoir pour systèmes d'imprimitivité les deux ensembles $\{1, 3, 5\}$ et $\{2, 4, 6\}$. Or 1 et 4 ne sont pas permutés par C, alors que l'un au moins des nombres 2, 3, 5, 6 fait partie du cycle C. Donc S et C sont forcément primitives et les deux cycles du sixième ordre S et C ont au plus quatre éléments communs ; si S et C ont 1, 2 ou 3 éléments communs, ils engendrent le groupe symétrique des substitutions des éléments qu'ils permutent et $(S, T, C) = \mathfrak{S}$. Supposons maintenant que S et C ont quatre éléments communs et que les éléments permutés par C sont 2, 3, 5, 6, 11, 12. Deux cas sont possibles. Ou bien S et C engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, 11, 12, d'où il résulte que $(S, T, C) = \mathfrak{S}$. Ou bien S et C engendrent un groupe simplement isomorphe à ${}_1G_{336}$ et qui contient l'une des deux substitutions $U = (1\ 5\ 3\ 12\ 2\ 11)$ ou $V = (1\ 5\ 3\ 11\ 2\ 12)$. Or, chacun des cycles U, V a un seul élément avec le cycle T et, par suite U et T aussi bien que V et T engendrent le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12. Il s'ensuit que $(S, T, C) = \mathfrak{S}$.

Le raisonnement est tout à fait analogue si le cycle C a des éléments communs seulement avec T, mais pas avec S.

Supposons maintenant que C a des éléments communs aussi bien avec S qu'avec T. C a alors au maximum quatre éléments communs avec l'un au moins des cycles S ou T. Supposons, pour fixer les idées, que C a au plus quatre éléments communs avec S. Comme le groupe (S, T, C) est primitif et que $\{1, 4\}$ est un système d'imprimitivité de S et T, $\{1, 4\}$ ne saurait être un système d'imprimitivité de S et C. Si S et C sont imprimitives, les cycles S et C ont alors trois éléments communs et ils ont pour systèmes d'imprimitivité les trois ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, $\{c, d, e\}$, où c, d, e sont trois nombres permutés par C qui ne font pas partie de S (et qui peuvent faire partie de T ou non). Dans ce cas S et C engendrent un groupe simplement isomorphe à ${}_1G_{162}$, groupe qui contient en tout cas la substitution $U = (1\ 2\ 5\ 6\ 3\ 4)$. Or

U a deux éléments communs avec T et est primitif avec T. Donc U et T engendrent le groupe symétrique $\mathfrak{S}_{10}$ et, par suite, $(S, T, C) = \mathfrak{S}$. Supposons maintenant que S et C sont primitives. Alors, si S et C ont un seul, deux ou trois éléments communs, ils engendrent toujours le groupe symétrique des substitutions des éléments qu'ils permutent. Et si S et C ont quatre éléments communs, alors ou bien S et C engendrent le symétrique des substitutions des éléments qu'ils permutent ou bien S et C engendrent un groupe simplement isomorphe à ${}_1G_{336}$, groupe qui contient la substitution $U = (1\ 3\ 2\ 6\ b\ 4)$, où b désigne un nombre >6 permuté par C. Or les cycles U et T ont deux ou, au maximum, trois éléments communs et ils sont primitifs. Ils engendrent donc toujours le groupe symétrique des substitutions des éléments qu'ils permutent. Il s'ensuit qu'en tous ces cas $(S, T, C) = \mathfrak{S}$. Le lemme 5 est donc démontré.

Corollaire 3. Quel que soit le cycle du sixième ordre C connexe et primitif avec ${}_2G_{1920}$ ou avec ${}_3G_{1920}$, en composant C avec les substitutions de ${}_2G_{1920}$ ou de ${}_3G_{1920}$, on obtient le groupe symétrique $\mathfrak{S}$ des substitutions des éléments permutés par C et par les substitutions de ${}_2G_{1920}$ respectivement de ${}_3G_{1920}$.

Démonstration. Posons $R = (7\ 8)$, $R' = (7\ 9)$, $RCR^{-1} = C'$, $R'CR'^{-1} = C''$, $({}_2G_{1920}, C) = G$, $({}_3G_{1920}, C) = G_1$. Nous savons que $R\,{}_2G_{1920}R^{-1} = {}_1G_{1920}$ et que $R'\,{}_3G_{1920}R'^{-1} = {}_2G_{1920}$. Donc les groupes $({}_1G_{1920}, C')$ et $({}_2G_{1920}, C)$ d'une part et les groupes $({}_2G_{1920}, C'')$ et $({}_3G_{1920}, C)$ d'autre part sont simplement isomorphes, ces quatre groupes sont du même degré et chacun d'eux est transitif et primitif. Or, d'après le lemme 5, le groupe $({}_1G_{1920}, C')$ est le symétrique des substitutions des éléments permutés par C' et les substitutions de ${}_1G_{1920}$. Il s'ensuit que G est le symétrique des substitutions des éléments permutés par C et les substitutions de ${}_2G_{1920}$ et que G_1 est le symétrique des substitutions des éléments permutés par C et les substitutions de ${}_3G_{1920}$, c. q. f. d.

Lemme 6. Soient $m \geq 2$ et $n \geq m$ deux entiers, soit G un groupe transitif et primitif de substitutions de degré n qui permutent les éléments de l'ensemble $E = \{1, 2, \ldots, n\}$, groupe qui contient un cycle d'ordre m: $C = (c_1 c_2 \ldots c_m)$. Alors les transformées de C par toutes les substitutions du groupe G constituent un système connexe et primitif de cycles d'ordre m qui permutent les n nombres $1, 2, \ldots, n$.

Démonstration. Soit G un groupe qui satisfait aux conditions de l'énoncé, soit N l'ordre de G et soit

1) $S_1 = 1$, $S_2, \ldots, S_N$ une suite formée de toutes les substitutions de G. Soit 2) $C_i = S_i C S_i^{-1}$, $i = 1, 2, \ldots, N$. Posons $G_1 = (C_1, C_2, \ldots, C_N)$.

Montrons d'abord que les cycles 2) permutent tous les éléments de l'ensemble E et qu'ils constituent un système connexe.

A cet effet, il suffit de remarquer que le groupe G_1 est engendré par une classe de substitutions conjuguées de G et, par suite, que G_1 est un sous-groupe distingué de G. Or on sait [6]) que tout sous-groupe distingué d'un groupe primitif de substitutions est transitif. Donc le groupe G_1 est transitif et ses substitutions permutent tous les éléments de l'ensemble E. Or, si les cycles 2) ne permutaient pas tous les éléments de l'ensemble E et s'ils ne formaient pas un système connexe, ils engendreraient un sous-groupe intransitif de G, ce qui est contradictoire. Notre assertion est donc démontrée.

Montrons maintenant que le système 2) est primitif. En effet supposons le contraire. Comme le système 2) est connexe et qu'il est composé de cycles du même ordre m, il existe alors un entier h diviseur de m et tel que si $m = m'h$ et si $C_i = (c_{i1}\, c_{i2} \ldots c_{im})$, $i = 1, 2, \ldots, N$, les ensembles

7) $E_{iq} = \{c_{iq}, c_{i\,q+h}, \ldots, c_{i\,q+(m'-1)\,h}\}$, $q = 1, 2, \ldots, h$, $i = 1, 2, \ldots, N$) [7]),

constituent les systèmes d'imprimitivité des cycles 2). Mais alors le groupe G est imprimitif et admet également les ensembles 7) pour systèmes d'imprimitivité. En effet, soit S une substitution quelconque de G, et soient E_{iq} et E_{jq}, deux systèmes d'imprimitivité quelconques des cycles 2). Montrons que si S transforme au moins un élément de E_{iq} en un élément de E_{jq}, alors S transforme tout l'ensemble E_{iq} en l'ensemble $E_{jq'}$. En effet, on a $C_i = S_i C S_i^{-1}$, $C_j = S_j C S_j^{-1}$. Comme G est un groupe, $S S_i$ est une substitution de G et il existe un indice ϱ, tel que $1 \leq \varrho \leq N$ et que $S S_i = S_\varrho$. On a donc $S C_i S^{-1} = C_\varrho = (c_{\varrho 1}\, c_{\varrho 2} \ldots c_{\varrho m})$. Comme tous les éléments de E_{iq} sont permuté par C_i et que S transforme au moins un élément de E_{iq} en un élément de E_{jq}, le cycle C_ρ permute au moins un élément de $E_{jq'}$ et on peut toujours choisir les notations de façon a avoir $c_{\varrho 1} \in E_{jq'}$. Comme C_ϱ est un cycle du système 2) que ce système 2 est imprimitif et que $E_{jq'}$ est un de ses systèmes d'imprimitivité, on doit avoir $\{c_{\varrho 1}, c_{\varrho\, 1+h}, \ldots, c_{\varrho\, 1+(m'-1)h}\} = E_{jq'}$. Or, S transforme un élément de E_{iq} en $c_{\varrho 1}$ et le cycle C_i en C_ϱ, deux éléments consécutifs dans C_i étant transformés par S en deux élé-

[6]) Voir, par exemple, *W. Burnside*, Theory of groups of finit order, Second Edition, Cambridge 1911, th. X, p. 196.

[7]) Ensembles qui ne sont pas tous distincts, mais dont deux quelconques sont soit disjoints soit confondus.

ments consécutifs dans C_ϱ. Donc S transforme nécessairement $E_{i\varrho}$ en $E_{j\varrho'}$. Cela étant quelle que soit la substitution S du groupe G ainsi que les systèmes d'imprimitivité $E_{i\varrho}$ et $E_{j\varrho'}$ du système 2), il s'ensuit que le groupe G est imprimitif et admet les mêmes systèmes d'imprimitivité que le système 2). Or ceci contredit notre hypothèse que le groupe G est primitif. Donc le système 2) est bien primitif et le lemme 6 est démontré.

Démonstration de la proposition I. Soit G un groupe transitif et primitif de substitutions des éléments $1, 2, \ldots, n$ qui contient deux cycles connexes et imprimitifs du sixième ordre C_1 et C_2 tels que $C_2 \neq C_1^j$, $j = \pm 1$. Il s'agit de montrer que G est le groupe symétrique $\mathfrak{S}$ des substitutions des éléments $1, 2, \ldots, n$.

D'après le § 2 du présent travail, C_1 et C_2 engendrent un groupe Γ simplement isomorphe à l'un des groupes G_{18}, G_{36}, ${}_1G_{162}$, G_{24}, G_{192} ou ${}_1G_{1920}$.

D'après le lemme 6, l'ensemble des cycles transformés de C_1 par toutes les substitutions de G constituent un système connexe et primitif de cycles du sixième ordre, qui permutent les n nombres $1, 2, \ldots, n$. Formons avec tous ces cycles une suite

$$1) \qquad \sigma_1 = C_1, \sigma_2, \ldots, \sigma_N \qquad (N = \text{ordre de } G, \ N > 1) \ ,$$

telle que, quel que soit l'entier $i \geq 2$, σ_i a au moins un élément commun avec l'un au moins des cycles $\sigma_1, \sigma_2, \ldots, \sigma_{i-1}$. Supprimons dans la suite 1) tout cycle σ_j $(j \geq 2)$, pour lequel il existe un indice j', tel que $1 \leq j' \leq j - 1$ et que $\sigma_j = \sigma_{j'}^h$, où $h = 1$ ou -1, et soit

2) $C_1' = C_1, C_2', \ldots, C_{N'}'$ la suite restante. Comme le système 1) est connexe et primitif, il en est de même du système 2). Du fait que le système 2) est primitif il résulte qu'il existe un indice $\varrho > 1$, tel que les cycles $C_1', C_2', \ldots, C_{\varrho-1}'$ constituent un système imprimitif alors que $C_1', C_2', \ldots, C_\varrho'$ forment un système primitif. Deux cas sont à distinguer.

a) $\varrho = 2$. Alors, d'après les lemmes 1—5 et les corollaires 1—3, les trois cycles C_1', C_2', C_2 qui forment un système connexe et primitif engendrent le groupe symétrique des substitutions des éléments qu'ils permutent. Formons maintenant avec les cycles 2) et C_2 une nouvelle suite 3) $C_1', C_2', C_2, C_3', \ldots, C_{N'}'$ et supprimons dans la suite 3) tout cycle, à partir du quatrième, qui ne permute aucun élément laissé fixe par tous les cycles qui le précèdent dans la suite 3).

Soit 4) $C_1', C_2', C_2, C_{i_1}', C_{i_2}', \ldots, C_{i_t}'$ la suite restante. D'après ce qui précède, les cycles 4) forment un système connexe et permutent,

les n nombres $1, 2, \ldots, n$. Or, d'après le lemme II de Hoyer, comme les trois cycles C'_1, C'_2, C_2 engendrent le symétrique des substitutions des éléments qu'ils permutent, il en est de même des quatre cycles C'_1, C'_2, C_2, C'_{i_1}, etc. ainsi que de l'ensemble des cycles $C'_i, C'_2, C_2, C'_{i_1}, \ldots, C'_{i_t}$. Or $G_1 = (C'_1, C'_2, C_2, C'_{i_1}, \ldots, C'_{i_t})$ est le groupe symétrique des substitutions de tous les éléments permutés par les substitutions de G et, comme $G_1 \subset C$, il s'ensuit que $G = G_1$. Donc G est bien le symétrique des substitutions des éléments $1, 2, \ldots, n$.

b) $\varrho > 2$. Alors les cycles 5) $C'_1 = C_1, C'_2, \ldots, C'_{\varrho-1}$ forment un système connexe et imprimitif dont les systèmes d'imprimitivité comprennent soit trois soit deux éléments chacun. Par définition de la suite 2), C'_ϱ a au moins un élément commun avec l'un au moins des cycles $C'_1, C'_2, \ldots, C'_{\varrho-1}$. Soit C'_j $(1 \leq j \leq \varrho - 1)$ un cycle de 5) qui a au moins un élément commun avec C'_ϱ et soit C'_l $(l \neq j)$ un cycle de 5) qui a au moins un élément commun avec C'_j. Un tel cycle C'_l existe en tout cas puisque $\varrho > 2$ et que le système 5) est connexe. Les deux cycles C'_j, C'_l sont connexes et imprimitifs alors que les trois cycles C'_j, C'_l, C'_ϱ forment un système connexe et primitif. Donc, d'après les lemmes 1—5 et les corollaires 1—3, le groupe (C'_j, C'_l, C'_ϱ) est le symétrique des substitutions des éléments permutés par les trois cycles C'_j, C'_l, C'_ϱ. Formons maintenant avec les cycles du système 2) une nouvelle suite 6) $C'_j, C'_l, C'_\varrho, C'_{i_4}, C'_{i_5}, \ldots, C'_{i_{N'}}$, telle que chaque cycle de cette suite à partir du second a au moins un élément commun avec l'un au moins des cycles qui le précèdent, ce qui est toujours possible, puisque le système 2) est connexe. Supprimons dans la suite 6) tout cycle à partir du quatrième (s'il y en a) qui ne permute aucun élément laissé fixe par tous les cycles de la suite 6) qui précèdent, dans cette suite, le cycle considéré. Soit 7) $C'_j, C'_l, C'_\varrho, C'_{k_1}, C'_{k_2}, \ldots, C'_{k_t}$ la suite restante. Les cycles 7) forment un système connexe et primitif et ils permutent le même ensemble d'éléments que les substitutions de G. Et comme le groupe (C'_j, C'_l, C'_ϱ) est le symétrique des substitutions des éléments permutés par les trois cycles C'_j, C'_l, C'_ϱ, il résulte du lemme II de Hoyer que le groupe $G_1 = (C'_j, C'_l, C'_\varrho, C'_{k_1}, \ldots, C'_{k_t})$ est le symétrique des substitutions de tous les éléments permutés par les substitutions de G. Or $G_1 \subset G$. Il s'ensuit que $G_1 = G$ et, par suite, G est bien le groupe symétrique des substitutions de tous les éléments qui sont permutés par les substitutions de G.

La proposition I est donc démontrée.

§ 4. Les divers groupes que peut engendrer un système connexe et primitif de cycles du sixième ordre

Proposition II. Quel que soit l'entier $k \geq 2$ *et quels que soient les* k *cycles du sixième ordre* $C_1, C_2, \ldots, C_k$ *qui forment un système connexe et primitif, le groupe* $(C_1, C_2, \ldots, C_k)$ *est soit simplement isomorphe à l'un des trois groupes* G_{120}, ${}_1G_{42}$, ${}_1G_{336}$, *soit le symétrique des substitutions des éléments permutés par tous les cycles du système considéré.*

La démonstration de la proposition II repose sur la proposition I et sur les lemmes suivants.

Lemme 7. Quel que soit le cycle du sixième ordre $C = (c_1 c_2 c_3 c_4 c_5 c_6)$ *connexe et primitif avec le groupe* G_{120}, *mais ne faisant pas partie de ce groupe, en composant* C *avec les substitutions de* G_{120}, *on obtient le groupe symétrique* $\mathfrak{S}$ *des substitutions des éléments permutés par* C *et toutes les substitutions de* G_{120}.

Démonstration. On a $G_{120} = (S, T)$, où $S = (1\,2\,3\,4\,5\,6)$, $T = (1\,2\,4\,3\,6\,5)$, donc $(S, T, C) = (G_{120}, C)$. Pour démontrer le lemme 7, il nous suffira dont de montrer que $(S, T, C) = \mathfrak{S}$. Comme le cycle C est connexe avec le groupe G_{120}, C permute l'un au moins des nombres 1, 2, 3, 4, 5, 6.

Six cas sont à distinguer.

1) C permute les six nombres 1, 2, 3, 4, 5, 6. Alors si C et S sont imprimitifs, on a $(S, T, C) = \mathfrak{S}_6$, d'après la proposition I, car alors (S, T, C) est un groupe primitif qui contient deux cycles connexes et imprimitifs du sixième ordre. Et si C est primitif avec S, comme $C \bar{\in} G_{120}$, $(S, C) = \mathfrak{S}_6$, d'après le § 2.

2) C permute cinq des nombres 1, 2, 3, 4, 5, 6 et le nombre 7. S et C sont alors en tout cas primitifs et engendrent soit le groupe $\mathfrak{S}_7$, auquel cas le lemme est démontré, soit l'un des deux groupes ${}_1G_{42}$, ${}_2G_{42}$. Or le groupe ${}_1G_{42}$ contient la substitution $U = (1\,3\,4\,2\,5\,7)$ et on a $(T^4U)^4 = (1\,2\,3) = A$, $(A, S) = \mathfrak{S}_6$ et $(\mathfrak{S}_6, C) = \mathfrak{S}_7 = (S, T, C)$. D'autre part, ${}_2G_{42}$ contient la substitution $V = (1\,4\,2\,3\,5\,7)$ et on a $(T^2V)^5 = (1\,6) = B$, $(B, S) = \mathfrak{S}_6$ et $(\mathfrak{S}_6, C) = \mathfrak{S}_7 = (S, T, C)$.

3) C permute quatre des nombres 1, 2, 3, 4, 5, 6 et les deux nombres 7 et 8. Alors, si S et C sont imprimitives on a $(S, T, C) = \mathfrak{S}_8$, d'après la proposition I. Et si S et C sont primitives, elles engendrent soit le groupe $\mathfrak{S}_8$, auquel cas le lemme est démontré, soit l'un des deux groupes ${}_1G_{336}$, ${}_2G_{336}$. Or le groupe ${}_1G_{336}$ contient la substitution $U = (1\,4\,3\,7\,8\,2)$

et on a $(T^2U)^3 = (1\ 6)$, donc $(S, T, C) = \mathfrak{S}_8$. Et le groupe ${}_2G_{336}$ contient la substitution $V = (1\ 4\ 3\ 8\ 7\ 2)$, $(T^2V)^3 = (1\ 6)$, donc $(S, T, C) = \mathfrak{S}_8$.

4) C permute trois des nombres 1, 2, 3, 4, 5, 6 et les trois nombres 7, 8, 9. Alors, si S et C sont imprimitives, $(S, T, C) = \mathfrak{S}_9$, d'après la proposition I, et, si S et C sont primitives, on a $(S, C) = \mathfrak{S}_9$, d'après le § 2. Donc aussi $(S, T, C) = \mathfrak{S}_9$.

5) C permute deux des nombres 1, 2, 3, 4, 5, 6 et les quatre nombres 7, 8, 9, 10. Alors, si S et C sont imprimitives, $(S, T, C) = \mathfrak{S}_{10}$, d'après la proposition I, et, si S et C sont primitives, $(S, C) = \mathfrak{S}_{10} = (S, T, C)$, d'après le § 2.

6) C permute un des nombres 1, 2, 3, 4, 5, 6 et les cinq nombres 7, 8, 9, 10, 11. Alors S et C sont toujours primitives et $(S, C) = \mathfrak{S}_{11} = (S, T, C)$, d'après le § 2.

Le lemme 7 est donc démontré.

Lemme 8. Quel que soit le cycle $C = (c_1c_2c_3c_4c_5c_6)$ *du sixième ordre, connexe avec le groupe* ${}_1G_{42}$ *et ne faisant pas partie des groupes* $(8h)\ {}_1G_{336}(8h)$, $h \geqslant 8$, *en composant* C *avec les substitutions de* ${}_1G_{42}$, *on obtient le groupe symétrique* $\mathfrak{S}$ *des substitutions des éléments permutés par* C *et par les substitutions de* ${}_1G_{42}$.

Démonstration. On a ${}_1G_{42} = (S, T)$, où $S = (1\ 2\ 3\ 4\ 5\ 6)$, $T = (1\ 3\ 4\ 2\ 5\ 7)$, donc $({}_1G_{42}, C) = (S, T, C)$. Comme C est connexe avec ${}_1G_{42}$, C est connexe avec l'une au moins des substitutions S, T. Le groupe $G = (S, T, C)$ est en tout cas primitif. Donc, d'après la proposition I, si G contient deux cycles connexes et imprimitifs du sixième ordre, on a $G = \mathfrak{S}$. Aussi nous nous bornerons à envisager le cas où les deux cycles S, C respectivement T, C pour autant qu'ils sont connexes, sont primitifs. Cinq cas sont alors à distinguer.

1) C permute les six nombres 1, 2, 3, 4, 5, 6 et les deux cycles S et C sont primitifs. Alors S et C engendrent soit le groupe $\mathfrak{S}_6$, auquel cas $(S, T, C) = \mathfrak{S}_7$, soit le groupe G_{120}, groupe qui contient la substitution $U = (1\ 2\ 4\ 3\ 6\ 5)$, et on a alors $(T^2U)^4 = (2\ 5\ 4)$, donc $(S, T, C) = \mathfrak{S}_7$.

2) C permute cinq des nombres 1, 2, 3, 4, 5, 6 et un nombre c de l'ensemble $\{7, 8\}$. Alors si $C \overline{\in} {}_2G_{336}$, comme $C \overline{\in} {}_1G_{336}$ par hypothèse, S et C engendrent, d'après le § 2, le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c et $(S, T, C) = \mathfrak{S}$. Et si $C \in {}_2G_{336}$,

comme $C \bar{\in} {}_1G_{336}$, S et C engendrent un groupe simplement isomorphe à ${}_1G_{42}$ et qui contient l'une des deux substitutions $U = (1\ 2\ 4\ 7\ 6\ 3)$ ou $V = (1\ 2\ 6\ 3\ 8\ 5)$. Or $(T^2U)^5 = (3\ 4)$ et $(TV)^5 = (2\ 4\ 6)$. Il en résulte que $(S, T, C) = \mathfrak{S}$.

3) C permute quatre nombres de la suite 1, 2, 3, 4, 5, 6 ainsi que les deux nombres c et d $(c<d)$ formant l'un des couples $\{7, 8\}$, $\{7, 9\}$, $\{8, 9\}$ ou $\{9, 10\}$ et C est primitif avec S. Si $c = 7$ et $d = 8$ et si $C \bar{\in} {}_2G_{336}$, S et C engendrent le groupe $\mathfrak{S}_8$ et $(S, T, C) = \mathfrak{S}_8$. Ou bien $C \in {}_2G_{336}$ et alors $(S, C) = {}_2G_{336}$, groupe qui contient la substitution $U = (1\ 4\ 3\ 8\ 7\ 2)$, on a $(T^3U^2)^5 = (2\ 7)$ et, par suite, $(S, T, C) = \mathfrak{S}$. Si $c = 7$ et $d = 9$, comme $C \bar{\in} (8\ 9)\, {}_1G_{336}\, (8\ 9)$ et $C \bar{\in} {}_1G_{336}$ les deux substitutions S et C engendrent soit le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, 7, 9 et, par suite, $(S, T, C) = \mathfrak{S}$, soit le groupe $(8\ 9)\, {}_2G_{336}\, (8\ 9)$, groupe qui contient la substitution $U = (1\ 2\ 5\ 6\ 7\ 9)$ et on a $(TU)^{10} = (1\ 5\ 6)$, donc $(S, T, C) = \mathfrak{S}$. Et si $c = 8$, $d = 9$ ou si $c = 9$, $d = 10$, alors S et C engendrent soit le symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, c, d soit un groupe simplement isomorphe à ${}_1G_{336}$ et qui contient l'une des deux substitutions $U = (1\ 2\ 5\ 6\ c\ d)$, $V = (1\ 2\ 5\ 6\ d\ c)$ et on a $(T^5U)^5 = (1\ 3\ 4)$, $(T^5V)^5 = (1\ 3\ 4)$. Donc dans tous ces cas, $(S, T, C) = \mathfrak{S}$.

4) C permute trois, deux ou un seul nombre de la suite 1, 2, 3, 4, 5, 6 et S et C sont primitifs. Alors S et C engendrent toujours, d'après le § 2, le groupe symétrique des substitutions de tous les éléments qu'ils permutent et $(S, T, C) = \mathfrak{S}$.

5) C ne permute aucun des nombres 1, 2, 3, 4, 5, 6. Comme C est connexe avec le groupe ${}_1G_{42}$, C permute alors nécessairement le nombre 7. Soient 8, 9, 10, 11, 12 les cinq autres nombres permutés par C. Alors T et C engendrent, d'après le § 2, le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 et, par suite, $(S, T, C) = \mathfrak{S}_{12}$.

Le lemme 8 est donc démontré.

Corollaire 4. Quel que soit le cycle C du sixième ordre, connexe et primitif avec ${}_2G_{42}$ et qui ne fait pas partie des groupes $(8h)\, {}_2G_{336}(8h)$, $h \geq 8$, en composant C avec les substitutions de ${}_2G_{42}$, on obtient le groupe symétrique $\mathfrak{S}$ des substitutions des éléments permutés par C et par les substitutions de ${}_2G_{42}$.

Démonstration. Ce corollaire résulte aussitôt du lemme 8 et du fait que ${}_2G_{42} = R\, {}_1G_{42} R^{-1}$, ${}_2G_{336} = R\, {}_1G_{336} R^{-1}$, où $R = (2\ 4\ 3)(6\ 7)$, et que ${}_2G_{42} \subset (8h)\, {}_2G_{336}\, (8h)$.

Lemme 9. Quel que soit le cycle du sixième ordre $C = (c_1 c_2 c_3 c_4 c_5 c_6)$, *connexe et primitif avec le groupe* ${}_1G_{336}$ *mais ne faisant pas partie de ce groupe, en composant* C *avec les substitutions de* ${}_1G_{336}$, *on obtient le groupe symétrique des substitutions des éléments permutés par* C *et les substitutions de* ${}_1G_{336}$.

Démonstration. On a ${}_1G_{336} = (S, T)$, où $S = (1\ 2\ 3\ 4\ 5\ 6)$ et $T = (1\ 4\ 3\ 7\ 8\ 2)$, donc $({}_1G_{336}, C) = (S, T, C)$. Posons $(S, T, C) = G$. Pour démontrer le lemme 9, il suffit de montrer que $G = \mathfrak{S}$. Le groupe G est primitif puisque ${}_1G_{336}$ est un groupe primitif de degré 8 et que C est un cycle du sixième ordre connexe avec ${}_1G_{336}$. Si l'un au moins des couples S, C ou T, C est imprimitif, $G = \mathfrak{S}$, d'après la proposition I.

Supposons d'abord que le cycle C a des éléments communs avec un seul des deux cycles S, T. Si c'est avec S seulement, les éléments communs à C et à T font alors partie de l'ensemble $\{5, 6\}$ et, si les cycles S et C sont primitifs, ils engendrent d'après le § 2 le groupe symétrique des substitutions des éléments permutés par S et C. Et si le cycle C a des éléments communs avec T, mais pas avec S, ces éléments communs font partie de l'ensemble $\{7, 8\}$; si donc T et C sont primitifs, ils engendrent le groupe symétrique des substitutions des éléments qu'ils permutent. Il s'entuit dans les deux cas que $G = \mathfrak{S}$.

Supposons maintenant que le cycle T a des éléments communs aussi bien avec S qu'avec T. Le groupe $(S, T) = {}_1G_{336}$ qui est trois fois transitif contient des cycles du sixième ordre qui permutent six quelconques des nombres 1, 2, 3, 4, 5, 6, 7, 8. Supposons d'abord que $C \bar{\epsilon} \mathfrak{S}_8$ et que C permute au moins un nombre > 8. Alors le groupe (S, T) contient un cycle du sixième ordre C_2 qui a au plus trois et au moins un élément commun avec C. Si C et C_2 sont imprimitifs, $(S, T, C) = \mathfrak{S}$, d'après la proposition I. Et, si C et C_2 sont primitifs, ils engendrent, d'après le § 2, le groupe symétrique des substitutions des éléments qu'ils permutent, et par suite $(S, T, C) = \mathfrak{S}$. Supposons maintenant que C a des éléments communs avec S et avec T et que $C \epsilon \mathfrak{S}_8$. Si C permute cinq nombres de la suite 1, 2, 3, 4, 5, 6 et le nombre 7, S et C sont alors primitifs et engendrent soit le groupe $\mathfrak{S}_7$ soit le groupe ${}_2G_{42}$ qui contient la substitution $U = (1\ 2\ 4\ 7\ 6\ 3)$ et $(T^4 U)^3 = (3\ 8)$. Si C permute cinq nombres de la suite 1, 2, 3, 4, 5, 6 et le nombre 8, S et C sont aussi primitifs et engendrent soit le groupe symétrique des substitutions des éléments 1, 2, 3, 4, 5, 6, 8, soit le groupe $(7\ 8)\,{}_1G_{42}(7\ 8)$, groupe qui contient la substitution $V = (1\ 3\ 2\ 6\ 8\ 4)$ et alors $(T^2 V)^5 = (3\ 4)$. Et, si C permute quatre nombres de la suite 1, 2, 3, 4, 5, 6 et les deux

nombres 7 et 8, alors si S et C sont imprimitifs, $(S, T, C) = \mathfrak{S}$, d'après la proposition I. Et si S et C sont primitifs, ils engendrent soit le groupe $\mathfrak{S}_8$ soit le groupe ${}_2G_{336}$, groupe qui contient la substitution $W = (1\ 2\ 5\ 6\ 7\ 8)$ et, dans ce dernier cas, $(T^2W)^3 = (3\ 8)$. Il en résulte que, dans tous ces cas, $(S, T, C) = \mathfrak{S}_8$.

Le lemme 9 est donc démontré.

Corollaire 5. Quel que soit le cycle $C = (c_1 c_2 c_3 c_4 c_5 c_6)$ connexe et primitif avec le groupe ${}_2G_{336}$ mais qui ne fait pas partie de ce groupe, en composant C avec les substitutions de ${}_2G_{336}$, on obtient le groupe symétrique des substitutions des éléments de l'ensemble $\{1, 2, 3, 4, 5, 6, 7, 8\} + \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

Démonstration. Le corollaire 5 est une conséquence immédiate de la relation ${}_2G_{336} = (7\ 8)\ {}_1G_{336}\ (7\ 8)$ et du lemme 9.

Proposition II. *Tout système connexe et primitif S de cycles du sixième ordre qui ne contient aucun couple de cycles connexes et imprimitifs engendre soit un groupe d'ordre 120, de degré 6, simplement isomorphe à G_{120}, soit un groupe d'ordre 42 et de degré 7, simplement isomorphe à ${}_1G_{42}$, soit un groupe d'ordre 336 et de degré 8, simplement isomorphe à ${}_1G_{336}$, soit le groupe symétrique $\mathfrak{S}$ des substitutions de tous les éléments permutés par les cycles du système considéré.*

Démonstration. Soit k un entier ≥ 2 et soit S un système connexe et primitif composé de k cycles du sixième ordre, système qui ne contient aucun couple de cycles connexes et imprimitifs. Formons avec tous les cycles du système S une suite

$$1)\quad C'_1, C'_2, \ldots, C'_k$$

telle que C'_1 est un cycle quelconque de S et, quel que soit l'indice $i \geq 2$, C'_i est un cycle du système S qui a au moins un élément commun avec l'un au moins des cycles $C'_1, C'_2, \ldots, C'_{i-1}$. Il est toujours possible de former une telle suite, puisque le système S est connexe.

Supprimons dans la suite 1) tout cycle C'_i $(i \geq 2)$, tel que

$$C'_i \in (C'_1, C'_2, \ldots, C'_{i-1})$$

et soit

$$2)\quad C_1, C_2, \ldots, C_{k'}$$

la suite restante. Il est clair que les cycles 2) permutent les mêmes éléments et engendrent le même groupe que les cycles du système S. Les

deux cycles C_1 et C_2 sont connexes et primitifs, d'après nos prémisses, ils engendrent donc, d'après le § 2, soit un groupe simplement isomorphe à l'un des trois groupes G_{120}, ${}_1G_{42}$, ${}_1G_{336}$, soit le groupe symétrique $\mathfrak{S}'$ des substitutions des éléments qu'ils permutent. Posons dans tous les cas $(C_1, C_2) = G$, et soit Γ le groupe engendré par tous les cycles du système S. Alors si $k' = 2$, on a $\Gamma = G$ et la proposition est démontrée.

Supposons que $k' > 2$.

Alors si G est d'ordre 120, il résulte du lemme 7, que le groupe (C_1, C_2, C_3) est le symétrique des substitutions des éléments permutés par les trois cycles C_1, C_2, C_3. Donc, d'après le lemme II de Hoyer, $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$.

Si G est d'ordre 336, il résulte du lemme 9, que (C_1, C_2, C_3) est alors en tous cas le symétrique des substitutions des éléments permutés par les trois cycles C_1, C_2, C_3 et, par suite $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$.

Si $G = \mathfrak{S}'$, on a $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$, d'après le lemme II de Hoyer.

Supposons enfin que G est d'ordre 42. Si le groupe (C_1, C_2, C_3) n'est pas de degré 8, d'après le lemme 8, c'est le symétrique des substitutions des éléments permutés par C_1, C_2 et C_3. Donc $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$. Et si le groupe (C_1, C_2, C_3) est de degré 8, il ressort de l'étude des groupes ${}_1G_{42}$, ${}_1G_{336}$ et du lemme 8 que le groupe (C_1, C_2, C_3) est soit le symétrique des substitutions des éléments permutés par C_1, C_2 et C_3, auquel cas $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$, soit un groupe simplement isomorphe à ${}_1G_{336}$; dans ce dernier cas, si $k' = 3$, on a $\Gamma = (C_1, C_2, C_3)$. Et si $k' > 3$ et le groupe (C_1, C_2, C_3) est d'ordre 336, d'après le lemme 9, le groupe (C_1, C_2, C_3, C_4) est alors nécessairement le symétrique des substitutions des éléments permutés par les quatre cycles C_1, C_2, C_3, C_4. Donc $(C_1, C_2, \ldots, C_{k'}) = \mathfrak{S}$.

La proposition II est donc démontrée.

Remarque 2. Il ressort de la démonstration des propositions I et II que tout système connexe et primitif de cycles du sixième ordre qui permutent, dans leur ensemble, un nombre ≥ 9 d'éléments engendre le groupe symétrique des substitutions de tous les éléments permutés par les cycles du système.

§ 5. Les bases du groupe symétrique $\mathfrak{S}_n$ de degré $n \geqslant 6$ dont l'une des substitutions est un cycle du sixième ordre

Soit n un entier ≥ 6, soit $\mathfrak{S}_n$ le groupe symétrique des substitutions des éléments $1, 2, \ldots, n$. Proposons nous maintenant de rechercher toutes les bases S, T du groupe $\mathfrak{S}_n$, dont l'une des substitutions T est

un cycle du sixième ordre. Nous verrons que, si $n \geq 9$, la condition nécessaire et suffisante pour que deux substitutions S, T du groupe $\mathfrak{S}_n$, dont l'une T est un cycle du sixième ordre, constituent une base de $\mathfrak{S}_n$, c'est que S et T soient connexes et primitives. Nous indiquerons aussi les conditions nécessaires et suffisantes pour que deux substitutions connexes S, T du groupe $\mathfrak{S}_n$ dont l'une T est un cycle du sixième ordre, soient imprimitives. Enfin nous donnerons des critères permettant de reconnaître toutes les bases des groupes $\mathfrak{S}_6$, $\mathfrak{S}_7$ et $\mathfrak{S}_8$ dont l'une des substitutions est un cycle du sixième ordre.

Lemme 10. Soient $m \geq 2$ et $n \geq m$ deux entiers et soient S et T deux substitutions connexes et primitives de degré n, dont l'une T est un cycle d'ordre m. Soit k l'ordre de S et soit $E = \{1, 2, \ldots, n\}$ l'ensemble des éléments permutés par S et T. Alors les k substitutions $S^i T S^{-i}$, $i = 0, 1, \ldots, k-1$, constituent toujours un système connexe et primitif de cycles qui permutent tous les éléments de l'ensemble E.

Démonstration. Soient S et T deux substitutions connexes et primitives de degré n qui permutent (ensemble) les éléments de l'ensemble $E = \{1, 2, \ldots, n\}$, soit k l'ordre de S et soit $T = (b_1 b_2 \ldots b_m)$.

Posons $T_i = S^i T S^{-i}$, $i = 0, 1, 2, \ldots, k-1$.

Soit j un élément quelconque de l'ensemble E. Montrons qu'il existe au moins une substitution T_i $(0 \leq i \leq k-1)$ qui permute j. En effet si j fait partie de l'ensemble $B = \{b_1, b_2, \ldots, b_m\}$, alors le cycle $T_0 = T$ permute j. Et si $j \bar{\in} B$, comme $j \in E$, j est permuté par S. Il existe dont un cycle $C = (a_1 a_2 \ldots a_h)$ de S, d'ordre $h \geq 2$, et un indice i' $(1 \leq i' \leq h)$, tel que $j = a_{i'}$. Comme les substitutions S et T sont connexes, un élément au moins de B fait partie de l'ensemble $A = \{a_1, a_2, \ldots, a_h\}$. Soit $a_{i''}$, un élément de A qui $\in B$ et soit $a_{i''} = b_t$ $(1 \leq t \leq m)$. Posons $u = i' - i''$, si $i' > i''$, et $u = i' - i'' + h$, si $i' < i''$. Alors $T_u = S^u T S^{-u}$ est un des cycles T_i qui permute j. En effet, soit b'_l l'élément que S^u substitue à b_l, quel que soit $l = 1, 2, \ldots, m$. On a $T_u = (b'_1 b'_2 \ldots b'_m)$ et $b'_t = j$.

Montrons maintenant que les cycles 1) $T_0, T_1, \ldots, T_k$ *constituent un système connexe.* En effet, supposons le contraire. Il existe alors un entier $r < k$ et r cycles

2) $T_{i_1} = T_0, \; T_{i_2}, \ldots, T_{i_r}$

de la suite 1), tels que ces r cycles constituent un système connexe alors que quel que soit le cycle $T_{i_{r+1}}$ de la suite 1) qui ne fait pas partie de 2), ce cycle ne permute aucun des éléments permutés par les cycles 2). Soit

E_1 l'ensembles des éléments permutés par les cycles 2). On a $E_1 \subset E$ mais $E_1 \neq E$. Soit $SE_1S^{-1} = E_2$. Les ensembles E_1 et E_2 sont disjoints. En effet supposons que $E_1E_2 \neq 0$ et soit a un élément commun à E_1 et à E_2. Les deux ensembles E_1 et E_2 sont évidemment d'égale puissance. Et s'il existait un élément b de E_2 qui $\bar{\epsilon}\, E_1$, il existerait un cycle de 1) étranger à 2) mais connexe avec le système 2). En effet, soit $T'_{i_l} = ST_{i_l}S^{-1}$, $l = 1, 2, \ldots, r$. Tous ces cycles font partie de la suite 1). Comme le système 2) est connexe, il en est de même du système 3) $T'_{i_1}, T'_{i_2}, \ldots, T'_{i_r}$ et E_2 est l'ensemble des éléments permutés par les cycles 3). Comme $E_1E_2 \neq 0$, et que chacun des deux systèmes 2) et 3) est connexe, les cycles des deux systèmes 2) et 3) constituent ensemble un système connexe et ce système contient au moins un cycle de la suite 1) qui ne fait pas partie de 2), puisque $b \epsilon E_2$ et $b \bar{\epsilon} E_1$, ce qui est en contradiction avec la définition de 2). Si donc $E_1E_2 \neq 0$, on a $E_2 \subset E_1$, et comme $\overline{\overline{E}}_1 = \overline{\overline{E}}_2$, on doit avoir $E_1 = E_2$. Mais alors, comme tous les éléments permutés par T font partie de E_1, chacune des substitutions S et T transforme l'ensemble E_1 en lui-même et, comme E_1 est un vrai sous-ensemble de E, S et T ne sauraient être connexes, ce qui est en contradiction avec les hypothèses faites sur S et T. Donc E_1E_2 est bien $= 0$. Posons $E_3 = SE_2S^{-1}$. Les deux ensembles E_2 et E_3 sont disjoints. En effet, s'il existait au moins un élément commun à E_2 et E_3 on devrait avoir $E_2 = E_3$, sinon il existerait un cycle de 1) ne faisant pas partie de 2), mais connexe avec 2) ce qui est contradictoire. Or on ne saurait avoir $E_2 = E_3$, puisque alors on devrait avoir $SE_1S^{-1} = E_2$, $SE_2S^{-1} = E_2$, ce qui est impossible, les ensembles E_1 et E_2 étant disjoints. Donc $E_2E_3 = 0$. Montrons maintenant que les ensembles E_1 et E_3 sont soit confondus soit disjoints. En effet, supposons que $E_1E_3 \neq 0$ et soit a un élément communs à E_1 et à E_3. Soit $T''_{i_l} = S^2T_{i_l}S^{-2}$, $l = 1, 2, \ldots, r$. Comme le système 2) est connexe, il en est de même de 4) $T''_{i_1}, T''_{i_2}, \ldots, T''_{i_r}$, les cycles 4) permutent les éléments de l'ensemble E_3 et comme $E_1E_3 \neq 0$, tous les cycles 2) et 4) ensemble forment un système connexe. Si donc E_3 contenait au moins un élément b étranger à E_1, il existerait un cycle de 4), donc aussi de 1), connexe avec 2), mais ne faisant pas partie de 2), ce qui contredit la définition de 2). Si donc $E_1E_3 \neq 0$, on a $E_3 \subset E_1$. Et comme $\overline{\overline{E}}_1 = \overline{\overline{E}}_3$, on a donc bien dans ce cas $E_1 = E_3$. Les ensembles E_1 et E_3 sont donc soit disjoints, soit confondus. Or si $E_1 = E_3$, on doit avoir $E = E_1 + E_2$, puisque chacune des deux substitutions S et T transforme l'ensemble $E_1 + E_2$ en lui-même et que S et T sont connexes.

Soit maintenant h un entier ≥ 2 et supposons que nous ayons déjà démontré que les ensembles $E_1, E_2 = SE_1S^{-1}, \ldots, E_h = SE_{h-1}S^{-1}$ sont disjoints deux à deux. Posons $E_{h+1} = SE_hS^{-1}$. Montrons que $E_iE_{h+1} = 0$, quel que soit $i = 2, 3, \ldots, h$, que E_1 et E_{h+1} sont soit disjoints, soit confondus et que si $E_1 = E_{h+1}$, alors $E = E_1 + E_2 + \cdots + E_h$. En effet, soit d'abord i un indice, tel que $2 \leq i \leq h$, et supposons que $E_iE_{h+1} \neq 0$. Alors on doit avoir $E_i = E_{h+1}$. En effet, les cycles 5) $S^{i-1}T_{il}S^{-i+1}$, $l = 1, 2, \ldots, r$, qui tous font partie de 1) constituent un système connexe et permutent les éléments de l'ensemble E_i. Les cycles 6) $S^hT_{il}S^{-h}$, $l = 1, 2, \ldots, r$, constituent également un système connexe de cycles appartenant à la suite 1) et les cycles 6) permutent les éléments de l'ensemble E_{h+1}. Si $E_iE_{h+1} \neq 0$, les cycles 5) et 6) ensembles constituent un système connexe qui permute tous les éléments de l'ensemble $E_1 + E_{h+1}$. Et si E_{h+1} contenait au moins un élément b étranger à E_i, les transformés des cycles 5) et 6) par S^{-i+1} formerait un système connexe de cycles appartenant à la suite 1) et comprenant tous les cycles de la suite 2) et au moins un cycle de 1) étranger à 2), ce qui est contradictoire. Si donc $E_iE_{h+1} \neq 0$, on doit avoir $E_{h+1} \subset E_i$ et comme $\overline{\overline{E}}_i = \overline{\overline{E}}_{h+1}$, on doit avoir $E_i = E_{h+1}$. Or, par définition de E_i, S transforme E_{i-1} en E_i. On doit donc avoir $E_{i-1} = E_{h+1}$ et $E_i = E_{h+1}$, ce qui est impossible puisque E_{i-1} et E_i sont, par hypothèse, disjoints. Donc $E_iE_{h+1} = 0$, $i = 2, 3, \ldots, h$. Quant aux deux ensembles E_1 et E_{h+1}, en répétant le raisonnement fait pour E_1 et E_3, on voit qu'ils sont soit confondus soit disjoints. Et comme S et T sont connexes, si $E_1 = E_{h+1}$, on doit alors avoir $E = E_1 + E_2 + \cdots + E_h$, puisque S aussi bien que T transforme l'ensemble $E_1 + E_2 + \cdots + E_h$ en lui-même. Si donc le système 1) n'est pas connexe, on peut en tout cas décomposer l'ensemble E en une somme de $\nu \geq 2$ sous-ensembles $E_1, E_2, \ldots, E_\nu$, disjoints deux-à-deux, d'égale puissance et tels que T transforme chacun de ces ensembles en lui-même, alors que S transforme E_1 en E_2, E_2 en $E_3, \ldots, E_\nu$ en E_1. Donc les deux substitutions S et T sont imprimitives et ont pour systèmes d'imprimitivité les ensembles $E_1, E_2, \ldots, E_\nu$. Or ceci contredit l'hypothèse que les deux substitutions S et T sont primitives. On voit donc que le système 2 est nécessairement connexe.

Montrons enfin que le système 1) est primitif. En effet supposons le contraire. Comme le système 1) est connexe et qu'il se compose de cycles qui sont tous du même ordre m, il existe donc un entier t, diviseur de m, tel que $2 \leq t < m$, $m = m't$ et que, quel que soit le cycle $T_i = (b_{i1}\, b_{i2}, \ldots\, b_{im})$, $i = 0, 1, \ldots, k-1$, du système 1), les ensembles

$E_{is} = \{b_{is}, b_{is+t}, \ldots, b_{is+(m'-1)t}\}$, $s = 1, 2, \ldots, t$, sont des systèmes d'imprimitivité de tous les cycles du système 1) tout système d'imprimitivité des cycles 1) étant, à son tour, un ensemble de la forme E_{is}. Soient E_1 et E_2 deux systèmes d'imprimitivité quelconques de l'ensemble des cycles 1) et supposons que S transforme au moins un élément de E_1 en un élément de E_2. Montrons que S transforme alors tout l'ensemble E_1 en E_2. En effet, comme E_1 est un système d'imprimitivité de l'ensemble des cycles 1), il existe deux entiers i et s, tels que $0 \leq i \leq k-1$, $1 \leq s \leq t$ et que $E_1 = \{b_{is}, b_{is+1}, \ldots, b_{is+(m'-1)t}\}$. Donc tous les éléments de l'ensemble E_1 sont permutés par le cycle $T_i = (b_{i1}\, b_{i2} \ldots b_{im})$ du système 1). Soit b_{is+jt} un élément de E_1 que S transforme en un élément u de E_2. Or, par définition de la suite 1), S transforme T_i en T_{i+1}, $i+1$ devant être remplacé par 0, si $i = k-1$, et $T_{i+1} = (b_{i+1\,1}, b_{i+1\,2} \ldots b_{i+1\,m})$. Comme S transforme b_{is+jt} en u, il doit exister un indice v $(1 \leq v \leq m)$, tel que $U = b_{i+1\,v}$ et, d'après ce qui précède, l'ensemble $E_2' = \{b_{i+1\,v}, b_{i+1\,v+t}, \ldots, b_{i+1\,v+(m'-1)t}\}$, où les indices $v+t, \ldots, v+(m'-1)t$ doivent être réduits modulo m de façon à être compris au sens large entre 1 et m, est un système d'imprimitivité de l'ensemble des cycles 1). Et comme S transforme T_i en T_{i+1} et b_{is+jt} en $b_{i+1\,v}$, $b_{is+jt+i}$ en $b_{i+1\,v+1}, \ldots, b_{is+jt+m-1}$ en $b_{i+1\,v+m-1}$, où les indices $>m$ doivent être réduits modulo m, on voit que S transforme E_1 en E_2'. Et comme E_2 et E_2' sont deux systèmes d'imprimitivité de l'ensemble des cycles 1) qui ont en commun l'élément u, on doit avoir $E_2 = E_2'$. On voit donc bien que si S transforme au moins un élément de E_1 en élément de E_2, S transforme tout l'ensemble E_1 en E_2. La substitution T jouit de la même propriété puisque $T = T_0$ est un cycle du système 1) qui est imprimitif et dont E_1 et E_2 sont deux systèmes d'imprimitivité quelconques. Donc les substitutions S et T sont imprimitives et admettent les mêmes systèmes d'imprimitivité que les cycles 1). Or ceci contredit notre hypothèse que S et T sont primitives.

Donc le système 1) est bien primitif et le lemme 10 est démontré.

Proposition III. Quel que soit l'entier $n \geq 9$, la condition nécessaire et suffisante pour que deux substitutions S, T du groupe symétrique $\mathfrak{S}_n$ d'ordre $n!$, dont l'une T est un cycle du sixième ordre, constituent une base de $\mathfrak{S}_n$, c'est que S et T soient connexes et primitives.

Démonstration. La condition est nécessaire. En effet, soit S, T une base du groupe $\mathfrak{S}_n$, dont l'une des substitutions T est un cycle du sixième ordre. On a donc $(S, T) = \mathfrak{S}_n$. Si S et T n'étaient pas connexes, le groupe (S, T) serait intransitif, ce qui est impossible puisque $\mathfrak{S}_n$ est

transitif. Donc S et T sont nécessairement connexes. Et, si S et T étaient imprimitives, le groupe (S, T) serait imprimitif, ce qui également est impossible, puisque le groupe $\mathfrak{S}_n$ est primitif. La condition énoncée est donc bien nécessaire.

La condition est suffisante. En effet, soient S et T deux substitutions connexes et primitives de degré $n \geq 9$ qui permutent, ensemble les n nombres $1, 2, \ldots, n$, soit T un cycle du sixième ordre et soit k l'ordre de la substitution S. Posons $T_i = S^i T S^{-i}$, $i = 0, 1, \ldots, k$. On a, en particulier, $T_0 = T$. D'après le lemme 10, les cycles $T_0, T_1, \ldots, T_m$ forment un système connexe et primitif de cycles du sixième ordre qui permutent les n nombres $1, 2, \ldots, n$ et, d'après la remarque 2, ces cycles engendrent le groupe symétrique $\mathfrak{S}_n$ des substitutions des éléments $1, 2, \ldots, n$. Donc $\mathfrak{S}_n \subset (S, T)$. Et comme on a évidemment $(S, T) \subset \mathfrak{S}_n$, il s'ensuit que $(S, T) = \mathfrak{S}_n$. Donc S, T est une base de $\mathfrak{S}_n$ et la condition énoncée est bien suffisante.

Les conditions nécessaires et suffisantes pour que deux substitutions connexes S et T, de degré n, dont l'une T est un cycle du sixième ordre, soient imprimitives.

Soit n un entier ≥ 6, soit S une substitution de degré n composée des h $(1 \leq h \leq 6)$ cycles $C_1, C_2, \ldots, C_h$, tels que $C_1 = (a_1 a_2 \ldots a_{m_1})$, $C_2 = (a_{m_1+1} \ldots a_{m_1+m_2}) \ldots$, $C_h = (a_{m_1+m_2+\cdots+m_{h-1}+1} \ldots a_{m_1+m_2\cdots+m_h})$, $m_1 + m_2 + \cdots + m_h = n$, et soit $T = (b_1 b_2 b_3 b_4 b_5 b_6)$, où b_1, b_2, b_3, b_4, b_5, b_6 sont six nombres de la suite $a_1, a_2, \ldots, a_n$, dont l'un au moins appartient à chaque cycle de S.

Nous utiliserons les notations suivantes. Si deux éléments b_i, b_j permutés par T font partie d'un même cycle C_l $(1 \leq l \leq h)$ d'ordre m_l de S et si $C_l = (a_{u+1} a_{u+2} \ldots a_{u+m_l})$ où $u = m_1 + \cdots + m_{l-1}$, $a_v = b_i$, $a_w = b_j$, $u + 1 \leq v \leq u + m_l$, $u + 1 \leq w \leq u + m_l$, nous désignerons par le symbole $\overline{b_i b_j}^{C_l}$ ou, pour abréger, simplement par $\overline{b_i b_j}$ et nous appellerons distance de b_i à b_j dans le cycle C_l le plus petit entier positif, tel que $v + \overline{b_i b_j} \equiv w \pmod{m_l}$.

D'autre part, quel que soit l'élément a_r du cycle C_l $(u+1 \leq l \leq u+m_l)$ et quel que soit l'entier k, nous désignerons par le symbole a_{r+k} l'élément a_s du cycle C_l, tel que $u + 1 \leq s \leq u + m_l$ et que $s \equiv r + k \pmod{m_l}$.

Soit j, k, l, m, n, p, q une permutation quelconque des nombres $1, 2, 3, 4, 5, 6$ et soit $b_j = a_{i_j}$, $b_k = a_{i_k}$, $b_l = a_{i_l}$, $b_m = a_{i_m}$, $b_p = a_{i_p}$ et $b_q = a_{i_q}$.

Les conditions suivantes sont nécessaires et suffisantes pour que les deux substitutions S et T soient imprimitives.

I. Si S se compose d'un seul cycle $C_1 = (a_1 a_2 \dots a_n)$ d'ordre n qui contient tous les éléments permutés par la substitution $T = (b_1 b_2 b_3 b_4 b_5 b_6)$ et si $b_j = a_{i_j}$ $(j = 1, 2, 3, 4, 5, 6)$, pour que S et T soient imprimitives, il faut et il suffit que l'une (au moins) des trois conditions suivantes soit satisfaite :

$$1. \quad D(\overline{b_1 b_2}, \overline{b_1 b_3}, \overline{b_1 b_4}, \overline{b_1 b_5}, \overline{b_1 b_6}, n) > 1 ,$$

$$2. \quad \overline{b_1 b_4} = \overline{b_4 b_1}, \ \overline{b_2 b_5} = \overline{b_5 b_2}, \ \overline{b_3 b_6} = \overline{b_6 b_3} ,$$

$$3. \quad n \equiv 0 \pmod 3, \quad \{a_{i_1}, a_{i_1+n/3}, a_{i_1+2n/3}\} = \{b_1, b_3, b_5\}$$

et

$$\{a_{i_2}, a_{i_2+n/3}, a_{j_2+2n/3}\} = \{b_2, b_4, b_6\} \quad \text{où} \quad a_{i_1} = b_1 , \quad a_{i_2} = b_2 .$$

II. Si S contient deux cycles $C_1 = (a_1 a_2 \dots a_m)$ et $C_2 = (a_{m_1+1} \dots a_{m_1+m_2})$, trois cas sont à distinguer.

IIa) L'un des deux cycles C_1, C_2 contient un seul des éléments permutés par T et le second des deux cycles C_1, C_2 contient cinq éléments permutés par T. Soit b_j l'élément de T permuté par le cycle C_λ et soient b_k, b_l, b_m, b_p, b_q les cinq éléments de T permutés par C_μ, où $\{\lambda, \mu\} = \{1, 2\}$. Alors la condition nécessaire et suffisante pour que S et T soient imprimitives, c'est que $D(\overline{b_k b_l}, \overline{b_k b_m}, \overline{b_k b_p}, \overline{b_k b_q}, m_1, m_2) > 1$.

IIb) L'un des deux cycles C_1, C_2 contient deux éléments permutés par T et le second des deux cycles C_1, C_2 contient quatre de ces éléments. Soit C_λ le cycle de S qui permute les deux éléments b_j, b_k de T et soit C_μ le cycle de S qui permute les quatre autres éléments b_l, b_m, b_p, b_q de T. Alors pour que S et T soient imprimitives, il faut et il suffit que l'on ait soit

$$1. \quad D(\overline{b_j b_k}, \overline{b_l b_m}, \overline{b_l b_p}, \overline{b_l b_q}, m_1, m_2) > 1 ,$$

soit

$$2. \quad \overline{b_j b_k} = \overline{b_k b_j}, \ \overline{b_l b_m} = \overline{b_m b_l}, \ \overline{b_p b_q} = \overline{b_q b_p} ,$$

les ensembles $\{j, k\}$, $\{l, m\}$, $\{p, q\}$ étant, à l'ordre près, $\{1, 4\}$, $\{2, 5\}$ et $\{3, 6\}$.

IIc) Chacun des cycles C_1, C_2 contient trois éléments permutés par T. Soit C_λ le cycle de S qui permute les trois éléments b_j, b_k, b_l de T et soit C_μ le cycle de S qui permute les trois éléments b_m, b_p et b_q de T. Alors pour que S et T soient imprimitives, il faut et il suffit que soit

1. $D(\overline{b_j b_k}, \overline{b_j b_l}, \overline{b_m b_p}, \overline{b_m b_q}, m_1, m_2) > 1$
soit

2. que $\{j, m\}$, $\{k, p\}$ et $\{l, q\}$ étant, à l'ordre près, les couples $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, que $m_1 = m_2$, $\overline{b_j b_k} = \overline{b_m b_p}$, $\overline{b_j b_l} = \overline{b_m b_q}$.

Soit 3. que $\{j, k, l\}$ et $\{m, p, q\}$ étant, à l'ordre près, les ensembles $\{1, 3, 5\}$ et $\{2, 4, 6\}$, que $m_1 \equiv 0 \pmod 3$, $m_2 \equiv 0 \pmod 3$, $\{a_{i_j}, a_{i_j + m_\lambda/3}, a_{i_j + 2m_\lambda/3}\} = \{b_j, b_k, b_l\}$, $\{a_{i_m}, a_{i_m + m_\mu/3}, a_{i_m + 2m_\mu/3}\} = \{b_m, b_p, b_q\}$, où $a_{i_j} = b_j$, $a_{i_m} = b_m$.

III. Si S contient trois cycles

$C_1 = (a_1 a_2 \ldots a_{m_1})$, $C_2 = (a_{m_1+1} \ldots a_{m_1+m_2})$, $C_3 = (a_{m_1+m_2+1} \ldots a_{m_1+m_2+m_3})$,

trois cas sont à distinguer.

IIIa) Deux cycles de S contiennent chacun un élément permuté par T et le troisième cycle de S contient quatre éléments permutés par T. Soit $b_j \in C_\lambda$, $b_k \in C_\mu$, et soient b_l, b_m, b_p, b_q les quatre éléments permutés par T qui font partie du cycle C_ν de S, $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$. Alors pour que S et T soient imprimitives, il faut et il suffit que soit

1. $D(\overline{b_l b_m}, \overline{b_l b_p}, \overline{b_l b_q}, m_1, m_2, m_3) > 1$, soit 2. que $\{j, k\}$, $\{l, m\}$, $\{p, q\}$ étant, à l'ordre près, les trois ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, que $m_\lambda = m_\mu$, $\overline{b_l b_m} = \overline{b_m b_l}$, $\overline{b_p b_q} = \overline{b_q b_p}$.

IIIb) Un cycle de S contient un seul élément permuté par T, un second cycle de S contient deux éléments permutés par T et le troisième cycle de S contient trois éléments permutés par T. Soit $b_j \in C_\lambda$, b_k et $b_l \in C_\mu$, b_m, b_p et $b_q \in C_\nu$. Alors pour que S et T soient imprimitives, il faut et il suffit que soit

1. $D(\overline{b_k b_l}, \overline{b_m b_p}, \overline{b_m b_q}, m_1, m_2, m_3) > 1$,

soit

2. que $\{i_j, i_k, i_l\}$ et $\{i_m, i_p, i_q\}$ étant à l'ordre près les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$ on ait $m_\mu = 2m_\lambda$, $\overline{b_m b_l} = \overline{b_l b_m}$, $m_\nu \equiv 0 \pmod 3$, $\{a_{i_m}, a_{i_m + m_\nu/3}, a_{i_m + 2m_\nu/3}\} = \{b_m, b_p, b_q\}$ où $a_{i_m} = b_m$.

IIIc) Chacun des trois cycles de S contient deux éléments permutés par T. Soient b_j et $b_k \in C_\lambda$, b_l et $b_m \in C_\mu$, b_p et $b_q \in C_\nu$. Pour que S et T soient imprimitives, il faut alors et il suffit que soit

1. $D(\overline{b_j b_k}, \overline{b_l b_m}, \overline{b_p b_q}, m_1, m_2, m_3) > 1$ soit 2. que $\{j, k\}$, $\{l, m\}$, $\{p, q\}$ étant, à l'ordre près, les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ l'on ait $\overline{b_j b_k} = \overline{b_k b_j}$, $\overline{b_l b_m} = \overline{b_m b_l}$, $\overline{b_p b_q} = \overline{b_q b_p}$, soit 3. que $\{j, k\}$, $\{l, p\}$, $\{m, q\}$ étant, à l'ordre près, les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, l'on ait $\overline{b_j b_k} = \overline{b_k b_j}$, $m_\mu = m_\nu$, $\overline{b_l b_m} = \overline{b_p b_q}$, soit 4. que $\{j, l, p\}$ et $\{k, m, q\}$ étant, à l'ordre près, les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, on ait $m_1 = m_2 = m_3$, $\overline{b_j b_k} = \overline{b_l b_m} = \overline{b_p b_q}$.

IV. Si S contient quatre cycles

$$C_1 = (a_1 a_2 \dots a_{m_1}), \quad C_2 = (a_{m_1+1} \dots a_{m_1+m_2}),$$
$$C_3 = (a_{m_1+m_2+1} \dots a_{m_1+m_2+m_3}), \quad C_4 = (a_{m_1+m_2+m_3+1} \dots a_{m_1+m_2+m_3+m_4}),$$

deux cas sont à distinguer.

IVa) Trois cycles de S contiennent chacun un seul élément permuté par T et le quatrième cycle de S contient trois éléments permutés par T. Soit $b_j \in C_\lambda$, $b_k \in C_\mu$, $b_l \in C_\nu$, b_m, b_p et $b_q \in C_\varrho$, $\{\lambda, \mu, \nu, \varrho\} = \{1, 2, 3, 4\}$. Pour que S et T soient imprimitives, il faut alors et il suffit que soit

1. $D(\overline{b_m b_p}, \overline{b_m b_q}, m_1, m_2, m_3, m_4) > 1$, soit 2. que $\{j, k, l\}$ étant l'un des deux ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, l'on ait $m_\lambda = m_\mu = m_\nu$, $m_\varrho \equiv 0 \pmod 3$, $\{a_{i_m}, a_{i_m+m_\varrho/3}, a_{i_m+2m_\varrho/3}\} = \{b_m, b_p, b_q\}$, où $a_{i_m} = b_m$.

IVb) Deux cycles de S contiennent chacun un élément permuté par T et les deux autres cycles de S contiennent chacun deux éléments permutés par T. Soit $b_j \in C_\lambda$, $b_k \in C_\mu$, b_l et $b_m \in C_\nu$, b_p et $b_q \in C_\varrho$. Alors pour que S et T soient imprimitives, il faut et il suffit que soit

1. $D(\overline{b_l b_m}, \overline{b_p b_q}, m_1, m_2, m_3, m_4) > 1$, soit 2. que $\{j, k\}$, $\{l, m\}$, $\{p, q\}$ étant, à l'ordre près, les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, on ait $m_\lambda = m_\mu$, $\overline{b_l b_m} = \overline{b_m b_l}$, $\overline{b_p b_q} = \overline{b_q b_p}$, soit 3. que, $\{j, k\}$, $\{l, p\}$, $\{m, q\}$ étant, à l'ordre près, les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, on ait $m_\lambda = m_\mu$, $m_\nu = m_\varrho$, $\overline{b_l b_m} = \overline{b_p b_q}$, soit 4, que $\{j, l, m\}$ et $\{k, p, q\}$ étant, à l'ordre près, les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, l'on ait $m_\nu = 2m_\lambda$, $m_\varrho = 2m_\mu$, $\overline{b_l b_m} = \overline{b_m b_l}$, $\overline{b_p b_q} = \overline{b_q b_p}$.

V. Si S contient cinq cycles

$$C_1 = (a_1 a_2 \dots a_{m_1}), \quad C_2 = (a_{m_1+1} \dots a_{m_1+m_2}),$$
$$C_3 = (a_{m_1+m_2+1} \dots a_{m_1+m_2+m_3}), \quad C_4 = (a_{m_1+m_2+m_3+1} \dots a_{m_1+m_2+m_3+m_4}),$$
$$C_5 = (a_{m+m_2+m_3+m_4+1} \dots a_{m_1+m_2+m_3+m_4+m_5}),$$

quatre cycles de S contiennent chacun un élément permuté par T, alors que le cinquième cycle de S contient deux élémnets permutés par T. Soit

$b_j \in C_\lambda$, $b_k \in C_\mu$, $b_l \in C_\nu$, $b_m \in C_\varrho$, b_p et $b_q \in C_\sigma$, $\{\lambda, \mu, \nu, \varrho, \sigma\} = \{1, 2, 3, 4, 5\}$

Pour que S et T soient imprimitives, il faut et il suffit que soit

1. $D(\overline{b_p b_q}, m_1, m_2, m_3, m_4, m_5) > 1$, soit
2. que, $\{j, k\}$, $\{l, m\}$, $\{p, q\}$ étant, à l'ordre près, les ensembles $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, on ait $m_\lambda = m_\mu$, $m_\nu = m_\varrho$, $\overline{b_p b_q} = \overline{b_q b_p}$, soit
3. que, $\{j, k, l\}$ et $\{m, p, q\}$ étant, à l'ordre près, les ensembles $\{1, 3, 5\}$, $\{2, 4, 6\}$, on ait $m_\lambda = m_\mu = m_\nu$, $m_\sigma = 2 m_\varrho$, $\overline{b_p b_q} = \overline{b_q b_p}$.

VI. Si S contient six cycles C_1, C_2, C_3, C_4, C_5, C_6 d'ordres respectifs m_1, m_2, m_3, m_4, m_5, m_6, chaque cycle de S contient un élément et un seul permuté par T. Soit $b_1 \in C_\lambda$, $b_2 \in C_\mu$, $b_3 \in C_\nu$, $b_4 \in C_\varrho$, $b_5 \in C_\sigma$ et $b_6 \in C_\varepsilon$, $\{\lambda, \mu, \nu, \varrho, \sigma, \varepsilon\} = \{1, 2, 3, 4, 5, 6\}$. Alors la condition nécessaire et suffisante pour que S et T soient imprimitives c'est que soit 1. $D(m_1, m_2, m_3, m_4, m_5, m_6) > 1$, soit 2. que $m_\lambda = m_\varrho$, $m_\mu = m_\sigma$, $m_\nu = m_\varepsilon$ soit 3. que $m_\lambda = m_\nu = m_\sigma$, $m_\mu = m_\varrho = m_\varepsilon$.

Les bases des groupes $\mathfrak{S}_6$, $\mathfrak{S}_7$ et $\mathfrak{S}_8$ dont l'une des substitutions est un cycle du sixième ordre.

Soit n un entier vérifiant les inégalités $6 \leq n \leq 8$, soit $\mathfrak{S}_n$ le groupe symétrique d'ordre $n!$ dont les substitutions permutent les éléments $1, 2, \ldots, n$, et soient S et T deux substitutions de $\mathfrak{S}_n$, dont l'une T est un cycle du sixième ordre. La condition que S et T soient connexes et primitives est alors nécessaire pour que S et T puissent constituer une base de $\mathfrak{S}_n$, mais cette condition n'est pas suffisante. Soit $T = (a_1 a_2 a_3 a_4 a_5 a_6)$. Distingons maintenant les cas où $n = 6$, 7 et 8.

1. *Soit* $n = 6$. Alors la condition nécessaire et suffisante pour que les deux substitutions S et T constituent une base de $\mathfrak{S}_6$, c'est que S et T soient connexes et primitives et que $S \neq T^i U^j T^{-i}$, où

$$\left.\begin{array}{ll} U = (a_1 a_2 a_4 a_3 a_6 a_5), & j = 1, 2, 3, 4, 5 \\ U = (a_1 a_3 a_5 a_2 a_6 a_4), & j = 1, 2 \\ U = (a_1 a_2 a_3 a_6 a_4), & j = 1, 2, 3, 4 \\ U = (a_1 a_2 a_3 a_5) \text{ ou } (a_1 a_2 a_6 a_3), & j = 1, 2, 3 \\ U = (a_1 a_2 a_5 a_4) \quad j = 1 & \end{array}\right\} i = 1, 2, 3, 4, 5, 6$$

$U = (a_1 a_5)(a_2 a_4)$, $j = 1$, $i = 1, 2, 3$.

2. *Soit* $n = 7$. Alors la condition nécessaire et suffisante pour que $(S, T) = \mathfrak{S}_7$, c'est que S et T soient connexes et primitives et que $S \neq T^i U^j T^{-i}$, où

$$\begin{aligned}
i &= 1, 2, 3, 4, 5, 6 \text{ et} \\
U &= (a_1 a_2 a_5 a_4 a_6 a_7 a_3) \text{ ou } (a_1 a_2 a_6 a_7 a_3 a_5 a_4), \quad j = 1 \\
U &= (a_1 a_2 a_6 a_3 a_7 a_5) \text{ ou } (a_1 a_2 a_4 a_7 a_6 a_3), \quad j = 1, 2, 3, 4. 5
\end{aligned}$$

a_7 désignant le nombre de la suite 1, 2, 3, 4, 5, 6, 7 qui n'est pas permuté par T.

3. *Soit* $n = 8$. Alors la condition nécessaire et suffisante pour que $(S, T) = \mathfrak{S}_8$, c'est que S et T soient connexes et primitives et que $S \neq R^k T^i U^j T^{-i} R^{-k}$, où $R = (a_7 a_8)$, $k = 1$ ou 2, $i = 1, 2, 3, 4, 5, 6$

$$\begin{aligned}
U &= (a_1 a_2 a_3 a_6 a_7 a_5 a_8 a_4), \ (a_1 a_2 a_4 a_3 a_5 a_6 a_7 a_8) \text{ ou } (a_1 a_2 a_5 a_3 a_7 a_8 a_6 a_4). \\
&\quad j = 1, 2, 3, 4, 5, 6, 7 \\
U &= (a_1 a_2 a_3 a_8 a_6 a_5 a_4 a_7), \quad j = 1, 2, 3 \\
U &= (a_1 a_2 a_3 a_7 a_4 a_6 a_8), \quad j = 1, 2, 3, 4, 5, 6 \\
U &= (a_1 a_2 a_5 a_6 a_8 a_7) \text{ ou } (a_1 a_3 a_5 a_7 a_6 a_8) \quad j = 1, 2, 3, 4, 5 \\
U &= (a_1 a_2 a_7 a_5 a_4 a_8), \quad j = 1, 2
\end{aligned}$$

a_7 et a_8 désignant les deux nombres de la suite 1, 2, 3, 4, 5, 6, 7, 8 qui ne sont pas permutés par T.

(Reçu le 14 avril 1949.)