Les substitutions qui sont des transformées réciproques.

Les substitutions qui sont des transformées réciproques[1]

Par SOPHIE PICCARD, Neuchâtel

1⁰ Soient S et T deux substitutions telles que $STS^{-1} = TST^{-1}$, les substitutions successives de la composition étant effectuées de droite à gauche. Nous appelons S et T des transformées réciproques. On voit immédiatement que deux substitutions qui sont des transformées réciproques sont semblables.

Il n'existe pas pour chaque substitution S une substitution $T \neq S$, telle que T et S soient des transformées réciproques. Par exemple, si S est une substitution circulaire d'ordre t et si t est un nombre premier, il n'existe aucune substitution $T \neq S$, telle que $STS^{-1} = TST^{-1}$.

Dans une première note[2]), nous avons établi la condition nécessaire et suffisante pour que deux substitutions *circulaires* soient des transformées réciproques. Ici nous établirons la condition nécessaire et suffisante pour que deux substitutions quelconques soient des transformées réciproques.

Notations. Quelle que soit la substitution R et quel que soit l'élément a de R, convenons de désigner par $[a]^R$ l'élément que R substitue à a.

Si S et T sont deux substitutions, telles que $STS^{-1} = TST^{-1}$, on a

$$T = S^{-1}\, TST^{-1}\, S.$$

Donc T est la transformée de S par $S^{-1}\,T$. Or, on sait que pour obtenir la transformée de S par $S^{-1}T$, il suffit d'effectuer la substitution $S^{-1}T$ sur les éléments de chaque cycle de S. Donc quel que soit le cycle $(a_1\, a_2 \ldots a_k)$ de S, T contient le cycle

$$\left([a_1]^{S^{-1}T}\ [a_2]^{S^{-1}T} \ldots\ [a_k]^{S^{-1}T}\right).$$

On en déduit immédiatement la

Proposition 1. Soient S et T deux transformées réciproques. Quel que soit l'élément a_1 de S, si α_1 est l'élément de T, tel que $[a_1]^T = [\alpha_1]^S$,

[1]) Une partie des résultats exposés dans cette note ont été présentés au Congrès international des mathématiciens, à Oslo.

[2]) Bulletin de la Société neuchâteloise des Sciences naturelles, tome 61, 1936.

le cycle C_1 de S qui contient a_1 et le cycle C_2 de T qui contient α_1 sont de même ordre et si l'on pose

$$C_1 = (a_1 a_2 \dots a_k),\ C_2 = (\alpha_1 \alpha_2 \dots \alpha_k),\ \text{on a}\ [a_i]^T = [\alpha_i]^S\ (i = 2, 3, \dots, k)\,.$$

Proposition 2. Soient S et T deux transformées réciproques portant sur les éléments d'un ensemble E. Soit a_1 un élément quelconque de E. Désignons par C_1 le cycle de S et par C_2 le cycle de T qui comprennent cet élément. Si l'on a $C_1 \neq C_2$, on a également $[a_1]^S \neq [a_1]^T$.

Démonstration. Posons $[a_1]^S = a_2$, $[a_1]^T = b_2$ et soit

$$C_1 = (a_1\, a_2\, a_3 \dots a_l)$$
$$C_2 = (a_1\, b_2\, b_3 \dots b_m)\,.$$

Supposons, contrairement à notre proposition, que $a_2 = b_2$.

On en déduit que

$$[b_2]^{STS^{-1}} = a_3\,,\ [a_2]^{TST^{-1}} = b_3\,.$$

Donc $a_3 = b_3$, puisque S et T sont des transformées réciproques. On en déduit de la même façon que $a_4 = b_4$ et ainsi de suite.

Finalement, il vient

$$a_k = b_k\ [k = \text{min.}\ (l; m)]\ \text{et}\ [b_k]^{STS^{-1}} = [a_k]^{TST^{-1}} = a_1\,.$$

Il en résulte que $C_1 = C_2$, ce qui est contraire à notre hypothèse. On ne saurait donc avoir $a_2 = b_2$, c. q. f. d.

Proposition 3. Si S et T sont des transformées réciproques, quelle que soit la substitution U des mêmes éléments, les substitutions $S_1 = USU^{-1}$ et $T_1 = UTU^{-1}$ sont également des transformées réciproques.

Démonstration. En effet, on a

$$S_1\, T_1\, S_1^{-1} = USU^{-1}\, UTU^{-1}\, US^{-1}\, U^{-1} = USTS^{-1}\, U^{-1}$$
$$T_1\, S_1\, T_1^{-1} = UTU^{-1}\, USU^{-1}\, UT^{-1}\, U^{-1} = UTST^{-1}\, U^{-1}$$

Et comme, par hypothèse, $STS^{-1} = TST^{-1}$, on a également

$$S_1 T_1 S_1^{-1} = T_1\, S_1\, T_1^{-1},\ \text{c. q. f. d.}$$

Corollaire 1. Soient S et T deux substitutions semblables. On peut toujours disposer des notations de façon à les écrire

$$S = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix} , \quad T = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_{i_1} & b_{i_2} & \dots & b_{i_n} \end{pmatrix} .$$

Soit S_1 une substitution quelconque des éléments $a_1, a_2, \dots, a_n$:

$$S_1 = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{j_1} & a_{j_2} & \dots & a_{j_n} \end{pmatrix} \quad \text{et soit} \quad T_1 = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_{j_1} & b_{j_2} & \dots & b_{j_n} \end{pmatrix} .$$

Nous dirons que les couples de substitutions S, S_1 et T, T_1 sont symétriques.

Montrons que si S et S_1 sont des transformées réciproques, T et T_1 le sont aussi.

En effet, soit
$$U = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} .$$
On a:
$$T = USU^{-1}, T_1 = US_1 U^{-1}.$$

Donc, en vertu de la proposition 3, si S et S_1 sont des transformées réciproques, T et T_1 le sont aussi, c. q. f. d.

Corollaire 2. Soient S et T deux transformées réciproques et soit U une substitution *permutable* avec S. Les substitutions S et $T_1 = UTU^{-1}$ sont alors également des transformées réciproques.

C'est une conséquence immédiate de la proposition 3, car la transformée de S par U coïncide, dans ce cas, avec S.

3⁰ Definition. Nous dirons que deux substitutions S et T composées des mêmes éléments formant un ensemble fini E sont *connexes*, s'il n'existe aucun sousensemble propre E_1 de E dont les éléments forment un système fini de cycles aussi bien dans S que dans T.

Si les substitutions S et T portant sur les mêmes éléments formant un ensemble E ne sont pas connexes, on peut évidemment toujours décomposer ces substitutions en un système de substitutions connexes.

Exemples. 1⁰ Soit $S = (12)(3)$ et $T = (13)(2)$. Ces deux substitutions sont connexes.

2⁰ Soit $S = (123)(45)(67)(89)$
$T = (12)(345)(6789)$.

Les substitutions S et T ne sont pas connexes, mais on peut décomposer S en deux substitutions $S_1 = (123)(45)$, $S_2 = (67)(89)$ et T en deux substitutions $T_1 = (12)(345)$, $T_2 = (6789)$, telles que les substitutions S_1 et T_1 sont connexes de même que les substitutions S_2 et T_2.

Proposition 4. La condition nécessaire et suffisante pour que deux substitutions S et T, portant sur les mêmes éléments formant un ensemble E, soient des transformées réciproques est que quelles que soient les substitutions connexes S_1 et T_1, telles que $S \supset S_1$ et $T \supset T_1$, les deux substitutions S_1 et T_1 soient des transformées réciproques.

Démonstration. La condition est nécessaire.

En effet, soit

$$STS^{-1} = TST^{-1} . \tag{I}$$

Soient S_1 et T_1 deux substitutions connexes quelconques, telles que $S \supset S_1$ et $T \supset T_1$. Appelons E_1 l'ensemble des éléments de chacune des substitutions S_1 et T_1; E_1 est un sous-ensemble de E.

Comme on sait, pour obtenir la transformée de la substitution T (S) par S (T), il suffit d'effectuer la substitution S (T) sur les éléments de chaque cycle de T (S). Or, comme les substitutions S_1 et T_1 sont connexes, lorsqu'on effectuera cette opération sur les cycles de T_1 (S_1), on obtiendra un système composé d'un nombre égal de cycles de mêmes ordres et composés uniquement d'éléments de E_1. Si donc l'égalité I) a lieu, on doit avoir

$$S_1 T_1 S_1^{-1} = T_1 S_1 T_1^{-1} . \tag{II}$$

La condition énoncée est donc bien nécessaire.

La condition est suffisante.

En effet, supposons qu'elle est satisfaite. Comme on voit sans peine, deux substitutions du même degré S et T, portant sur les mêmes éléments, peuvent toujours être décomposées, et cela de façon unique, en un nombre fini de substitutions

$$\begin{aligned} S &= S_1 + S_2 + \cdots + S_k , \\ T &= T_1 + T_2 + \cdots + T_k , \end{aligned}$$

de telle manière que les substitutions $S_1, S_2, \ldots, S_k$ soient sans éléments communs deux à deux, de même que les substitutions $T_1, T_2, \ldots, T_k$, et que les substitutions S_i et T_i soient connexes, quel que soit $i = 1, 2, \ldots, k$.

En vertu de notre hypothèse, $S_i T_i S_i^{-1} = T_i S_i T_i^{-1}$, quel que soit $i = 1, 2, \ldots, k$. Il s'agit de montrer que $STS^{-1} = TST^{-1}$. Or, on voit immédiatement que

$$STS^{-1} = S_1 T_1 S_1^{-1} + S_2 T_2 S_2^{-1} + \cdots + S_k T_k S_k^{-1}$$

et

$$TST^{-1} = T_1 S_1 T_1^{-1} + T_2 S_2 T_2^{-1} + \cdots + T_k S_k T_k^{-1}.$$

On a donc bien $STS^{-1} = TST^{-1}$, de sorte que la condition énoncée est suffisante, c. q. f. d.

Corollaire. Il résulte de la proposition 4 que l'étude des conditions nécessaires et suffisantes pour que deux substitutions S et T soient des transformées réciproques peut être limitée au cas où S et T sont connexes. C'est ce que nous supposerons toujours dans la suite.

Proposition 5[1]**.** La condition nécessaire et suffisante pour que deux substitutions connexes S et T de degré n, dont les éléments constituent un ensemble E, soient des transformées réciproques est qu'il existe un nombre impair α, tel que $n = k\alpha$ (k = entier $\geqslant 1$) et k suites $a_1^{(i)}, a_2^{(i)}, \ldots, a_\alpha^{(i)}$ comprenant tous les éléments de E, ainsi qu'un nombre entier fixe i_0 compris au sens large entre 1 et α, tels que dans les cycles de T figurent les successions d'éléments

$$\left.\begin{array}{l} a_1^{(1)} a_1^{(2)} \ldots a_1^{(k)} \\ a_2^{(1)} a_2^{(2)} \ldots a_2^{(k)} \\ \ldots\ldots\ldots\ldots \\ a_\alpha^{(1)} a_\alpha^{(2)} \ldots a_\alpha^{(k)} \end{array}\right\} \tag{1}$$

et

$$a^{(k)}_{1+l\cdot 2^k} \quad a^{(1)}_{i_0+l} \qquad (l = 0, 1, 2, \ldots, \alpha - 1) \tag{2}$$

et que dans les cycles de S figurent les successions d'éléments

$$\left.\begin{array}{llll} a_1^{(1)} a_\alpha^{(2)} & \ldots a^{(q+1)}_{2-2^q} & & \ldots a^{(k)}_{2-2^{k-1}} \\ a_2^{(1)} a_1^{(2)} & \ldots a^{(q+1)}_{3-2^q} & & \ldots a^{(k)}_{3-2^{k-1}} \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots & & \ldots\ldots\ldots \\ a_\alpha^{(1)} a_{\alpha-1}^{(2)} & \ldots a^{(q+1)}_{\alpha+1-2^q} & & \ldots a^{(k)}_{\alpha+1-2^{k-1}} \end{array}\right\} \tag{3}$$

et

$$a^{(k)}_{1+2^{k-1}+l\cdot 2^k} \quad a^{(1)}_{i_0+l} \qquad (l = 0, 1, 2, \ldots, \alpha - 1), \tag{4}$$

---

[1]) Les notations employées dans l'énoncé de ce théorème de même que les démonstrations des propositions 1, 2 et des corollaires de la proposition 3 ont été simplifiées d'après des remarques de M. B. L. van der Waerden.

les indices devant être réduits selon le module α de façon à être toujours compris au sens large entre 1 et α.

Démonstration. *La condition est nécessaire.*

Soient S et T deux substitutions connexes de degré n portant sur les éléments d'un ensemble E et soit I) $STS^{-1}=TST^{-1}$.

Soit $(a_1^{(1)}a_2^{(1)} \dots a_\alpha^{(1)})$ un cycle quelconque de la substitution $S^{-1}T$.

Comme $a_1^{(1)}, a_2^{(1)}, \dots, a_\alpha^{(1)}$ sont des éléments, distincts deux à deux, de l'ensemble E, on a $1 \leqslant \alpha \leqslant n$ et comme les éléments en question constituent un cycle de $S^{-1}T$, on a

$$[a_i^{(1)}]^T = [a_{i+1}^{(1)}]^S, \tag{5}$$

quel que soit $i = 1, 2, \dots, \alpha$, l'indice $i+1$ devant être remplacé par 1, si $i = \alpha$.

Je dis que les suites $[a_1^{(1)}]^T, [a_2^{(1)}]^T, \dots, [a_\alpha^{(1)}]^T$ et $a_1^{(1)}, a_2^{(1)}, \dots, a_\alpha^{(1)}$ sont disjointes ou sont composées des mêmes éléments.

En effet, supposons que ces suites ont un élément commun et soit, par exemple,

$$[a_i^{(1)}]^T = a_j^{(1)} (1 \leqslant i \leqslant \alpha, \ 1 \leqslant j \leqslant \alpha).$$

On a donc aussi, en vertu de (5), $[a_{i+1}^{(1)}]^S = a_j^{(1)}$.

Par conséquent, S contient dans un de ses cycles la succession d'éléments $a_{i+1}^{(1)} a_j^{(1)}$. Effectuons sur ces éléments la substitution T. Il vient $[a_{i+1}^{(1)}]^T [a_j^{(1)}]^T$, ou encore, en vertu de (5), $[a_{i+2}^{(1)}]^S [a_{j+1}^{(1)}]^S$.

Or, comme par hypothèse, l'égalité I) a lieu, la proposition 1 implique que T doit contenir dans un de ses cycles la succession d'éléments $a_{i+2}^{(1)} a_{j+1}^{(1)}$. Donc $[a_{i+2}^{(1)}]^T = a_{j+1}^{(1)}$.

Supposons à présent que pour un nombre entier g quelconque compris au sens large entre 1 et α, on a $[a_g^{(1)}]^T = a_r^{(1)}$. Montrons que $[a_{g+2}^{(1)}]^T = a_{r+1}^{(1)}$. Comme $[a_g^{(1)}]^T = a_r^{(1)}$, on a aussi, en vertu de (5), $[a_{g+1}^{(1)}]^S = a_r^{(1)}$. Donc S contient dans un de ses cycles la succession d'éléments $a_{g+1}^{(1)} a_r^{(1)}$. Effectuons sur ces éléments la substitution T. Il vient $[a_{g+1}^{(1)}]^T [a_r^{(1)}]^T$, ou encore, en vertu de (5), $[a_{g+2}^{(1)}]^S [a_{r+1}^{(1)}]^S$. Comme I) a lieu par hypothèse, il en résulte en vertu de la proposition 1, que T doit contenir dans un de ses cycles la succession d'éléments $a_{g+2}^{(1)} a_{r+1}^{(1)}$. On a donc bien $[a_{g+2}^{(1)}]^T = a_{r+1}^{(1)}$, c. q. f. d.

Par conséquent, si $[a_i^{(1)}]^T = a_j^{(1)}$, on a $[a_{i+2g}^{(1)}]^T = a_{j+g}^{(1)}$, quel que soit $g = 1, 2, \ldots, \alpha - 1$, les indices devant être réduits mod. α de façon à être compris au sens large entre 1 et α.

La suite $a_j^{(1)}, a_{j+1}^{(1)}, \ldots, a_\alpha^{(1)}, a_1^{(1)}, a_2^{(1)}, \ldots, a_{j-1}^{(1)}$ étant composée de α termes distincts, il doit en être de même de la suite $[a_i^{(1)}]^T$, $[a_{i+2}^{(1)}]^T$, $[a_{i+2\cdot 2}^{(1)}]^T, \ldots, [a_{i+2(\alpha-1)}^{(1)}]^T$. Il en résulte, d'une part, que les suites $[a_1^{(1)}]^T, [a_2^{(1)}]^T, \ldots, [a_\alpha^{(1)}]^T$ et $a_1^{(1)}, a_2^{(1)}, \ldots, a_\alpha^{(1)}$, si elles ne sont pas disjointes, sont bien composées des mêmes éléments et, d'autre part, que la suite des nombres $i, i+2, i+2\cdot 2, \ldots, i+2(\alpha-1)$, réduits mod. α de façon à être compris au sens large entre 1 et α, est composée de α nombres distincts: $1, 2, \ldots, \alpha$. Donc la suite des nombres $2, 2\cdot 2, \ldots, 2(\alpha-1)$, réduits mod. α, doit contenir $\alpha - 1$ termes distincts : $1, 2, \ldots, \alpha - 1$. Il en découle que α est un nombre *impair* (puisque tous les nombres $2, 2\cdot 2, \ldots, 2(\alpha-1)$ sont pairs).

En posant $[a_1^{(1)}]^T = a_{i_0}^{(1)}$, on voit que la condition énoncée est bien nécessaire dans notre cas particulier.

Si les suites $[a_1^{(1)}]^T, [a_2^{(1)}]^T, \ldots, [a_\alpha^{(1)}]^T$ et $a_1^{(1)}, a_2^{(1)}, \ldots, a_\alpha^{(1)}$ sont disjointes, posons $[a_i^{(1)}]^T = a_i^{(2)}$ $(i = 1, 2, 3, \ldots, \alpha)$.

En vertu des égalités 5), on a donc aussi

$$[a_{i+1}^{(1)}]^S = a_i^{(2)} \quad (i = 1, 2, \ldots, \alpha),$$

l'indice $i+1$ devant être remplacé par 1, si $i = \alpha$.

Ainsi T comprend dans ses cycles les successions d'éléments

$$\begin{array}{c} a_1^{(1)} a_1^{(2)} \\ a_2^{(1)} a_2^{(2)} \\ \cdots\cdots \\ a_\alpha^{(1)} a_\alpha^{(2)} \end{array}$$

et S comprend dans ses cycles les successions d'éléments

$$\begin{array}{c} a_1^{(1)} a_\alpha^{(2)} \\ a_2^{(1)} a_1^{(2)} \\ \cdots\cdots \\ a_\alpha^{(1)} a_{\alpha-1}^{(2)} \end{array}$$

Quel que soit le nombre entier i, compris au sens large entre 1 et α, si l'on effectue sur la succession $a_{i+1}^{(1)} a_i^{(2)}$ d'éléments de S (l'indice $i+1$ devant être remplacé par 1 si $i = \alpha$) la substitution T, il vient $a_{i+1}^{(2)} [a_i^{(2)}]^T$. Or, S substitue l'élément $a_{i+1}^{(2)}$ à $a_{i+2}^{(1)}$. Donc, comme T contient la succession d'éléments $a^{(1)}_{i+2}a^{(2)}_{i+2}$, en vertu de l'égalité I) et de la proposition 1, on doit avoir

$$[a^{(2)}_{i+2}]^S = [a^{(2)}_i]^T \qquad (i = 1, 2, \ldots, \alpha), \tag{6}$$

les indices $i+2$ devant être réduits mod. α de façon à être compris au sens large entre 1 et α.

Soit à présent q un nombre entier quelconque $\geqslant 1$ et $< \frac{n}{\alpha}$, soit $a^{(i)}_1$, $a^{(i)}_2, \ldots, a^{(i)}_\alpha (i = 1, 2, \ldots, q+1)$ $q+1$ suites comprenant ensemble $(q+1)\alpha$ éléments, distincts deux à deux, de l'ensemble E et supposons que T contient dans ses cycles les successions d'éléments

$$\left.\begin{matrix} a^{(1)}_1 a^{(2)}_1 \ldots a^{(q+1)}_1 \\ a^{(1)}_2 a^{(2)}_2 \ldots a^{(q+1)}_2 \\ \ldots\ldots\ldots\ldots\ldots \\ a^{(1)}_\alpha a^{(2)}_\alpha \ldots a^{(q+1)}_\alpha \end{matrix}\right\} \tag{1'}$$

que S contient dans ses cycles les successions d'éléments

$$\left.\begin{matrix} a^{(1)}_1 a^{(2)}_\alpha \ldots a^{(q+1)}_{2-2^q} \\ a^{(1)}_2 a^{(2)}_1 \ldots a^{(q+1)}_{3-2^q} \\ \ldots\ldots\ldots\ldots\ldots \\ a^{(1)}_\alpha a^{(2)}_{\alpha-1} \ldots a^{(q+1)}_{\alpha+1-2^q} \end{matrix}\right\} \tag{3'}$$

et que l'on a (7) $[a^{(q+1)}_j]^T = [a^{(q+1)}_{j+2^q}]^S$, quel que soit $j = 1, 2, \ldots \alpha$, les indices $j+2^q$ devant être réduits mod. α de façon à être compris au sens large entre 1 et α.

Montrons que la suite *) $[a^{(q+1)}_1]^T$, $[a^{(q+1)}_2]^T, \ldots, [a^{(q+1)}_\alpha]^T$ est soit composée des mêmes éléments que la suite $a^{(1)}_1, a^{(1)}_2, \ldots, a^{(1)}_\alpha$, soit ne possède aucun élément des suites **) $a^{(i)}_1, a^{(i)}_2, \ldots, a^{(i)}_\alpha (i=1, 2, \ldots, q+1)$.

En effet, supposons d'abord que la suite *) possède au moins un élément commun avec l'une des suites **) et soit, par exemple,

$$[a^{(q+1)}_{i'}]^T = a^{(r)}_{i''} \, (1 \leqslant i' \leqslant \alpha, \; 1 \leqslant i'' \leqslant \alpha, \; 1 \leqslant r \leqslant q+1).$$

Je dis que $r = 1$. En effet, supposons le contraire et soit $r > 1$.

Mais alors, comme T substitue, en vertu de nos supposition, $a_{i''}^{(r)}$ à $a_{i''}^{(r-1)}$, on doit avoir $a_{i'}^{(q+1)} = a_{i''}^{(r-1)}$. Or, c'est impossible car $r-1 \leqslant q$ et, par suite, les deux éléments $a_{i''}^{(r-1)}$ et $a_{i'}^{(q+1)}$ appartiennent à deux suites distinctes du système **). Or, d'après nos hypothèses, deux telles suites n'ont aucun élément commun. On a donc bien $r = 1$.

Comme $[a_{i'}^{(q+1)}]^T = a_{i''}^{(1)}$, on a, en vertu de 7), $[a_{i'+2^q}^{(q+1)}]^S = a_{i''}^{(1)}$.

Soit $i_1 (1 \leqslant i_1 \leqslant \alpha)$ le rang de la ligne du système 3') qui comprend l'élément $a_{i'+2^q}^{(q+1)}$. Le nombre i_1 est défini par l'égalité

$$i_1 + 1 - 2^q = i' + 2^q,$$

d'où l'on déduit

$$i_1 = i' - 1 + 2^{q+1},$$

ce nombre devant être réduit mod. α de façon à être compris au sens large entre 1 et α.

La substitution S contient donc dans un de ses cycles la succession d'éléments

$$a_{i_1}^{(1)} a_{i_1-1}^{(2)} \ldots a_{i'+2^q}^{(q+1)} a_{i''}^{(1)} a_{i''-1}^{(2)} \ldots a_{i''+1-2^q}^{(q+1)} .$$

En effectuant sur cette suite la substitution T, on trouve

$$a_{i_1}^{(2)} a_{i_1-1}^{(2)} \ldots [a_{i'+2^q}^{(q+1)}]^T a_{i''}^{(2)} a_{i''-1}^{(3)} \ldots [a_{i''+1-2^q}^{(q+1)}]^T .$$

Or, S substitue $a_{i_1}^{(2)}$ à $a_{i_1+1}^{(1)}$ et $a_{i''}^{(2)}$ à $a_{i''+1}^{(1)}$. Donc, puisque I) a lieu, en vertu de la proposition 1, T doit contenir la succession d'éléments

$$a_{i_1+1}^{(1)} a_{i_1+1}^{(2)} \ldots a_{i_1+1}^{(q+1)} a_{i''+1}^{(1)} a_{i''+1}^{(2)} \ldots a_{i''+1}^{(q+1)}$$

et, par conséquent, T substitue $a_{i''+1}^{(1)}$ à $a_{i_1+1}^{(q+1)} = a_{i'+2^{q+1}}^{(q+1)}$.

Donc, en vertu de 7), S substitue $a_{i''+1}^{(1)}$ à $a_{i'+2^q+2^{q+1}}^{(q+1)}$, les indices $i' + 2^{q+1}$ et $i' + 2^q + 2^{q+1}$ devant être réduits mod. α, de façon à être compris au sens large entre 1 et α.

Soit à présent l un nombre entier quelconque $\geqslant 1$ et $< \alpha - 1$, et supposons que $[a_{i'+l \cdot 2^{q+1}}^{(q+1)}]^T = a_{i''+l}^{(1)}$, donc aussi $[a_{i'+2^q+l \cdot 2^{q+1}}^{(q+1)}]^S = a_{i''+l}^{(1)}$. Montrons que $[a_{i'+(l+1)2^{q+1}}^{(q+1)}]^T = a_{i''+l+1}^{(1)}$, donc aussi $[a_{i'+2^q+(l+1)2^{q+1}}^{(q+1)}]^S = a_{i''+l+1}^{(1)}$.

Soit $i_{l+1} (1 \leqslant i_{l+1} \leqslant \alpha)$ le rang de la ligne du système 3') à laquelle appartient l'élément $[a_{i'+2^q+l \cdot 2^{q+1}}^{(q+1)}]^S$.

Le nombre i_{l+1} est défini par l'égalité

$$i_{l+1}+1-2^q=i'+2^q+l\cdot 2^{q+1},$$

d'où l'on déduit

$$i_{l+1}=i'-1+(l+1)\,2^{q+1},$$

ce nombre devant être réduit mod. α de façon à être compris au sens large entre 1 et α.

Il en résulte que S contient dans un de ses cycles la succession d'éléments

$$a^{(1)}_{i_{l+1}}\ a^{(2)}_{i_{l+1}-1}\dots\ a^{(q+1)}_{i'+2^q+l\cdot 2^{q+1}}\ a^{(1)}_{i''+l}\ a^{(2)}_{i''+l-1}\ \dots\ a^{(q+1)}_{i''+l+1-2^q}\ .$$

Effectuons sur cette suite la substitution T. Il vient

$$a^{(2)}_{i_{l+1}}\ a^{(3)}_{i_{l+1}-1}\ \dots\ [a^{(q+1)}_{i'+2^q+l\cdot 2^{q+1}}]^T\ a^{(2)}_{i''+l}\ a^{(3)}_{i''+l-1}\ \dots\ [a^{(q+1)}_{i''+l+1-2^q}]^T.$$

Or, S substitue

$$a^{(2)}_{i_{l+1}}\ \text{ à }\ a^{(1)}_{i_{l+1}+1}\ \text{ et }\ a^{(2)}_{i''+l}\ \text{ à }\ a^{(1)}_{i''+l+1}\ .$$

Donc comme I) a lieu, T doit contenir dans un de ses cycles, en vertu de la proposition 1, la succession d'éléments

$$a^{(1)}_{i_{l+1}+1}\ a^{(2)}_{i_{l+1}+1}\ \dots\ a^{(q+1)}_{i_{l+1}+1}\ \ a^{(1)}_{i''+l+1}\ \ a^{(2)}_{i''+l+1}\ \dots\ a^{(q+1)}_{i''+l+1}\ .$$

Donc T substitue

$$a^{(1)}_{i''+l+1}\ \text{ à }\ a^{(q+1)}_{i_{l+1}+1}=a^{(q+1)}_{i'+(l+1)\,2^{q+1}}\ .$$

On a donc bien

$$[a^{(q+1)}_{i'+(l+1)\,2^{q+1}}]^T=a^{(1)}_{i''+l+1}$$

et, par conséquent aussi, en vertu de 7),

$$[a^{(q+1)}_{i'+2^q+(l+1)\,2^{q+1}}]^S=a^{(1)}_{i''+l+1},\quad \text{c.q.f.d.}$$

La suite $a^{(1)}_{i''}$, $a^{(1)}_{i''+1}$, $\dots$, $a^{(1)}_{i''+\alpha-1}$ étant composée de α éléments distincts (à savoir $a^{(1)}_1$, $a^{(1)}_2$, $a^{(1)}_\alpha$), il doit en être de même de la suite

$$[a^{(q+1)}_{i'}]^T,\ [a^{(q+1)}_{i'+2^{q+1}}]^T,\ [a^{(q+1)}_{i'+2\cdot 2^{q+1}}]^T,\ \dots,\ [a^{(q+1)}_{i'+(\alpha-1)\,2^{q+1}}]^T,$$

donc aussi de la suite

$$i', i'+2^{q+1}, i'+2\cdot 2^{q+1}, \ldots, i'+(\alpha-1)2^{q+1},$$

les nombres de cette dernière suite devant être réduits mod. α, de façon à être compris au sens large entre 1 et α. Par conséquent, la suite des nombres $2^{q+1}, 2\cdot 2^{q+1}, \ldots, (\alpha-1)2^{q+1}$, réduits selon le mod. α, doit contenir $\alpha-1$ nombres distincts, à savoir $1, 2, \ldots, \alpha-1$.

Or, ceci n'est possible que si le nombre α est impair.

Posons

$$[a_1^{(q+1)}]^T = a_{i_0}^{(1)}.$$

Il vient

$$[a_{1+l\cdot 2^{q+1}}^{(q+1)}]^T = [a_{1+2^q+l\cdot 2^{q+1}}^{(q+1)}]^S = a_{i_0+l}^{(1)}, \tag{8}$$

quel que soit $l = 1, 2, \ldots, \alpha-1$.

Il ressort de ces considérations qu'effectivement la suite *) soit ne contient aucun élément des suites **), soit est composée des éléments de la suite $a_1^{(1)}, a_2^{(1)}, \ldots, a_\alpha^{(1)}$ et que dans ce dernier cas la condition énoncée est bien nécessaire.

Si les suites *) et **) sont disjointes, posons

$$[a_i^{(q+1)}]^T = a_i^{(q+2)} \qquad (i = 1, 2, \ldots, \alpha).$$

On a donc aussi, en vertu de (7) :

$$[a_{i+2^q}^{(q+1)}]^S = a_i^{(q+2)} \qquad (i = 1, 2, \ldots, \alpha).$$

Montrons que quel que soit le nombre entier i compris au sens large entre 1 et α, on a

$$[a_i^{(q+2)}]^T = [a_{i+2^{q+1}}^{(q+2)}]^S. \tag{9}$$

Comme nous venons de le voir, S contient dans un de ses cycles la succession d'éléments $a_{i+2^q}^{(q+1)}\, a_i^{(q+2)}$. Effectuons sur ces éléments la substitution T.

Il vient

$$a_{i+2^q}^{(q+2)}\, [a_i^{(q+2)}]^T.$$

Or, S substitue $\quad a_{i+2^q}^{(q+2)} \quad$ à $\quad a_{i+2^q+2^q}^{(q+1)} = a_{i+2^{q+1}}^{(q+1)}$.

Donc puisque I) a lieu, comme T contient dans un de ses cycles la succession d'éléments

$$a_{i+2^{q+1}}^{(q+1)}\, a_{i+2^{q+1}}^{(q+2)},$$

on doit avoir, en vertu de la proposition 1, $[a_{i+2^{q+1}}^{(q+2)}]^S = [a_i^{(q+2)}]^T$, c.q.f.d.

Montrons que $[a^{(q+1)}_{i+1-2^q}]^S = a^{(q+2)}_{i+1-2^{q+1}}$, quel que soit $i = 1, 2, \ldots, \alpha$. En effet, nous avons $[a^{(q+1)}_{i+2^q}]^S = a^{(q+2)}_i$, quel que soit $i = 1, 2, \ldots, \alpha$. Soit ϱ le nombre entier compris au sens large entre 1 et α et tel que

$$\varrho + 2^q = i + 1 - 2^q, \text{ ou encore } \varrho = i + 1 - 2^{q+1} (\text{mod. } \alpha) .$$

On a donc

$$[a^{(q+1)}_{i+1-2^q}]^S = [a^{(q+1)}_{\varrho+2^q}]^S = a^{(q+2)}_\varrho = a^{(q+2)}_{i+1-2^{q+1}}, \text{ c. q. f. d.}$$

Cela étant quel que soit le nombre entier $q = 1, 2, 3, \ldots$, il en résulte que le nombre n (degré des substitutions S et T) est un multiple de α. Soit $n = k\alpha$. (k = entier $\geqslant 1$.)

Donc les cycles de T contiennent bien les successions d'éléments du système 1) et les cycles de S les successions d'éléments du système 3).

D'autre part, les deux suites d'éléments

$$[a^{(k)}_1]^T, [a^{(k)}_2]^T, \ldots, [a^{(k)}_\alpha]^T$$

et

$$[a^{(k)}_{2-2^{k-1}}]^S, [a^{(k)}_{3-2^{k-1}}]^S, \ldots, [a^{(k)}_{\alpha+1-2^{k-1}}]^S$$

doivent, en vertu de ce qui précède, être composées des éléments $a^{(1)}_1, a^{(1)}_2, \ldots, a^{(1)}_\alpha$. Notamment, si l'on désigne par i_0 le nombre entier compris au sens large entre 1 et α et tel que $[a^{(k)}_1]^T = a^{(1)}_{i_0}$, il vient, en vertu de 8), où l'on pose $q = k - 1$,

$$[a^{(k)}_{1+l \cdot 2^k}]^T = [a^{(k)}_{1+2^{k-1}+l \cdot 2^k}]^S = a_{i_0+l} \qquad (l = 0, 1, 2, \ldots, \alpha - 1) ,$$

et le nombre α doit être impair.

La condition énoncée est donc bien nécessaire.

La condition est suffisante.

Soient S et T deux substitutions connexes de degré $n = k\alpha$, où α est un nombre entier impair et k un entier $\geqslant 1$, portant sur les éléments d'un ensemble E, et supposons qu'il existe k suites $a^{(i)}_1, a^{(i)}_2, \ldots, a^{(i)}_\alpha$ ($i = 1, 2, \ldots, k$), comprenant tous les éléments de E, et un nombre entier i_0 compris au sens large entre 1 et α, tels que dans les cycles de T figurent les successions d'éléments 1) et 2) et que dans les cycles de S figurent les successions d'éléments 3) et 4). Montrons que dans ce cas on a I) $STS^{-1} = TST^{-1}$.

On obtient, comme on sait, la transformée d'une substitution T (S) par S (T) en effectuant sur les éléments de chaque cycle de T (S) la substitution S (T).

Notre proposition sera établie si nous prouvons qu'à toute suite

$$a_i^{(1)} a_i^{(2)} \ldots a_i^{(q+1)} \ldots a_i^{(k)} \tag{i}$$

$(1 \leqslant i \leqslant \alpha)$ du système (1) correspond une suite déterminée du système 3), à savoir

$$a_{i-1}^{(1)} a_{i-2}^{(2)} \ldots a_{i-2^q}^{(q+1)} \ldots a_{i-2^{k-1}}^{(k)} \tag{i'}$$

(le nombre $i - 1$ devant être remplacé par α, si $i = 1$), telle que si l'on effectue sur la suite i) la substitution S et sur la suite i') la substitution T, on obtient dans les deux cas la même suite d'éléments de E, quel que soit $i = 1, 2, \ldots, \alpha$.

En effet, quel que soit le nombre entier q compris au sens large entre 1 et $k - 2$, il existe (par définition des systèmes 1) et 3)) un nombre entier u compris au sens large entre 1 et α, et tel que

$$i = u + 1 - 2^q \ (\mathrm{mod.}\ \alpha).$$

Donc

$$i - u - 1 + 2^q \equiv 0 \ (\mathrm{mod.}\ \alpha). \tag{10}$$

D'autre part, il existe un nombre entier l' $(0 \leqslant l' \leqslant \alpha - 1)$, tel que

$$i = 1 + 2^{k-1} + l' \cdot 2^k \ (\mathrm{mod.}\ \alpha).$$

D'où

$$i - 1 - 2^{k-1} - l' \cdot 2^k \equiv 0 \ (\mathrm{mod.}\ \alpha). \tag{11}$$

Il ressort de ces remarques et de la définition de S que S remplace

$$\begin{array}{lll} a_i^{(1)} & \text{par} & a_{i-1}^{(2)} \\ a_i^{(q+1)} & \text{par} & a_{u+1-2^{q+1}}^{(q+2)} \quad (1 \leqslant q \leqslant k-2) \\ a_i^{(k)} & \text{par} & a_{i_0+l'}^{(1)} \end{array}$$

D'autre part, il existe un nombre entier l'' $(0 \leqslant l'' \leqslant \alpha - 1)$, tel que

$$i - 2^{k-1} = 1 + l'' \cdot 2^k \ (\mathrm{mod.}\ \alpha).$$

D'où on déduit

$$i - 1 - 2^{k-1} - l'' \cdot 2^k \equiv 0 \ (\mathrm{mod.}\ \alpha). \tag{12}$$

De 11) et 12), il ressort que $l'' = l'$.

Il résulte de ces remarques et de la définition de T que T remplace

$$\begin{array}{lll} a^{(1)}_{i-1} & \text{par} & a^{(2)}_{i-1} \\ a^{(q+1)}_{i-2q} & \text{par} & a^{(q+2)}_{i-2q} \quad (1 \leqslant q \leqslant k-2) \\ a^{(k)}_{i-2^{k-1}} & \text{par} & a^{(1)}_{i_0+l'} \; . \end{array}$$

Or

$$i-2^q-[u+1-2^{q+1}] \equiv 0 \ (\text{mod. } \alpha) \, .$$

En effet, on en déduit $i - u - 1 + 2^q \equiv 0$ (mod. α), ce qui est bien vrai en vertu de 10).

Ainsi si l'on effectue sur la suite i) la substitution S et sur la suite i') la substitution T, on obtient dans les deux cas la même suite d'éléments de E.

Cela étant quel que soit $i = 1, 2, \ldots, \alpha$, on a donc bien I) $STS^{-1} = TST^{-1}$ et la condition énoncée est suffisante, c. q. f. d.

Corollaires.

1° Soient S et T deux substitutions connexes portant sur les mêmes éléments formant un ensemble E.

Si S et T sont des transformées réciproques, il résulte de ce qui précède, les notations étant les mêmes que ci-dessus, que la substitution $S^{-1}\,T$ est régulière d'ordre α *impair*, et qu'elle comprend les k cycles suivants:

$$(a_1^{(i)} \; a^{(i)}_{1+2^{i-1}} \; a^{(i)}_{1+2\cdot 2^{i-1}} \ldots a^{(i)}_{1+(\alpha-1)2^{i-1}}) \quad (i = 1, 2, \ldots, k) \, ,$$

les indices devant être réduits mod. α, de façon à être compris au sens large entre 1 et α.

La condition que $S^{-1}\,T$ soit régulière d'ordre impair est nécessaire mais pas suffisante pour que les substitutions T et S soient des transformées réciproques.

2° Soit $k = 1$. Dans ce cas $n = \alpha$ et la substitution $S^{-1}\,T$ est circulaire:

$$S^{-1}T = (a_1^{(1)} a_2^{(1)} \ldots a_\alpha^{(1)}) \, .$$

Quel que soit le nombre entier q compris au sens large entre 0 et $\alpha - 1$, on a alors

$$[a^{(1)}_{1+2\cdot q}]^T = [a^{(1)}_{2+2q}]^S = a^{(1)}_{i_0+q} \, ,$$

i_0 ayant la signification définie plus haut.

Comme $1 + 2(i_0 - 1) = i_0 + i_0 - 1$, on voit que T contient un cycle de premier ordre et un seul, à savoir $(a^{(1)}_{2i_0-1})$, de même que S, dont l'unique cycle de premier ordre est $(a^{(1)}_{2i_0-2})$.

Il ressort de la proposition 5 et de ces remarques que si les substitutions connexes S et T sont des transformées réciproques et si la substitution $S^{-1}T$ est circulaire, les substitutions S et T contiennent chacune un et un seul cycle de premier ordre, et inversément si les substitutions connexes S et T sont des transformées réciproques et contiennent chacune un et un seul cycle de premier ordre, la substitution $S^{-1}T$ est circulaire. Par contre, si la substitution $S^{-1}T$ est de degré $k \cdot \alpha$, où $k > 1$, α étant l'ordre de cette substitution, tous les cycles des transformées réciproques connexes S et T sont d'ordre $\geqslant k$, ces ordres ne pouvant être que des multiples de k, et inversément si l'ordre de chacun des cycles des substitutions S et T qui sont des transformées réciproques connexes, est > 1, la substitution $S^{-1}T$ n'est pas circulaire.

3° Si les transformées réciproques S et T sont régulières, elles sont composées chacune d'un nombre impair de cycles.

En effet, si les substitutions S et T sont des transformées réciproques, elles satisfont à la proposition 5. Soit m le nombre de cycles de S (T) et r l'ordre de cette substitution. On a donc $n = mr$, n étant le degré de la substitution S (T). De la proposition 5 on conclut, en employant les mêmes notations que ci-dessus, que $n = k \cdot \alpha$ et $r = r_1 k$, r_1 désignant un nombre entier $\geqslant 1$.

Donc
$$mr = mr_1 k = k\alpha.$$

On en déduit
$$\alpha = m\, r_1.$$

Or, α étant un nombre impair, il doit en être de même de m et de r_1. Par conséquent le nombre de cycles de chacune des substitutions S et T est bien impair, c. q. f. d.

(Reçu le 1er octobre 1936.)