Zeitschrift: Bulletin de la Société Neuchâteloise des Sciences Naturelles
Herausgeber: Société Neuchâteloise des Sciences Naturelles
Band: 61 (1936)

Artikel: Les transformées réciproques
Autor: Piccard, Sophie
DOI: https://doi.org/10.5169/seals-88724

Les transformées réciproques

PAR

SOPHIE PICCARD

INTRODUCTION

Nous dirons que deux substitutions S et T portant sur les mêmes éléments sont des *transformées réciproques* si l'on a

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

les substitutions successives de la composition étant effectuées de droite à gauche.

C'est à l'étude de ces substitutions qu'est consacrée la présente note.

Dans le premier chapitre, nous établissons la condition nécessaire et suffisante à laquelle doivent satisfaire deux substitutions circulaires pour être des transformées réciproques.

Le second chapitre traite des conditions nécessaires et suffisantes pour que deux substitutions de second et de troisième ordre soient des transformées réciproques.

On voit immédiatement que si deux substitutions sont des transformées réciproques, elles sont semblables.

Chapitre I

§ 1. Soit S et T deux substitutions circulaires de n éléments

$$S = (a_1\, a_2 \ldots a_n),\quad T = (a_{i_1}\, a_{i_2} \ldots a_{i_n}),$$

$i_1, i_2, \ldots, i_n$ étant une permutation des nombres $1, 2, \ldots, n$, et supposons que l'on a

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

Pour obtenir STS^{-1} (TST^{-1}), il suffit, comme on sait, d'effectuer sur le cycle de T (S) la substitution S (T), le résultat étant également une substitution circulaire.

Soit $$STS^{-1} = TST^{-1} = (a_{j_1}\, a_{j_2} \ldots a_{j_n}),$$

$j_1, j_2, \ldots, j_n$ étant une permutation des nombres 1, 2, ..., n, et supposons que S substitue à l'élément a_{i_1} l'élément a_{j_1}, tandis que T substitue à l'élément a_1 l'élément a_{j_1}. Pour qu'il en soit ainsi, il suffit de choisir convenablement les notations et cette hypothèse ne nuit pas à la généralité des raisonnements qui suivent.

On a donc (II) $$S = \begin{pmatrix} a_{i_1}\, a_{i_2} \ldots a_{i_n} \\ a_{j_1}\, a_{j_2} \ldots a_{j_n} \end{pmatrix} = (a_1\, a_2 \ldots a_n)$$

et (III) $$T = \begin{pmatrix} a_1\, a_2 \ldots a_n \\ a_{j_1}\, a_{j_2} \ldots a_{j_n} \end{pmatrix} = (a_{i_1}\, a_{i_2} \ldots a_{i_n}).$$

De (II), on déduit sans peine les égalités

$$a_{j_1} = a_{i_1+1},\ a_{j_2} = a_{i_2+1},\ \ldots,\ a_{j_n} = a_{i_n+1},$$

un indice $i_t + 1$ devant être remplacé par le reste de sa division par n, s'il est supérieur à n.

Il en résulte

$$\text{(IV)} \qquad \begin{cases} j_1 = i_1 + 1 \\ j_2 = i_2 + 1 \\ \cdots\cdots\cdots \\ j_n = i_n + 1, \end{cases}$$

les nombres $i_t + 1$ $(1 \leq t \leq n)$ devant être réduits mod. n, s'ils sont supérieurs à n.

De (III) on déduit :

$$a_{i_2} = a_{j_{i_1}},\ a_{i_3} = a_{j_{i_2}},\ \ldots,\ a_{i_n} = a_{j_{i_{n-1}}},\ a_{i_1} = a_{j_{i_n}},$$

d'où il résulte

$$\text{(V)} \qquad i_2 = j_{i_1},\ i_3 = j_{i_2},\ \ldots,\ i_n = j_{i_{n-1}},\ i_1 = j_{i_n}.$$

De (IV) et de (V) on déduit immédiatement

$$\text{(VI)} \qquad i_{i_1} + 1 = i_2,\ i_{i_2} + 1 = i_3,\ \ldots,\ i_{i_n} + 1 = i_1.$$

Les égalités (VI) constituent une condition nécessaire pour que les deux substitutions S et T soient des transformées réciproques. Montrons que cette condition est aussi suffisante.

Soit donc $S = (a_1\, a_2 \ldots a_n)$ et $T = (a_{i_1}\, a_{i_2} \ldots a_{i_n})$ deux substitutions circulaires des mêmes éléments, telles que les égalités (VI) soient satisfaites.

Montrons que l'on a (I) $STS^{-1} = TST^{-1}$.

Comme $i_1, i_2, \ldots, i_n$ est une permutation des nombres $1, 2, \ldots, n$, il existe, pour tout entier t compris au sens large entre 1 et n, un indice $l(t)$ $(1 \leq l(t) \leq n)$, tel que $t = i_{l(t)}$.

Donc $$S = (a_1 a_2 \ldots a_n) = (a_{i_{l(1)}} a_{i_{l(2)}} \ldots a_{i_{l(n)}}),$$

$$T = (a_{i_1} a_{i_2} \ldots a_{i_n}) = (a_{i_{i_{l(1)}}} a_{i_{i_{l(2)}}} \ldots a_{i_{i_{l(n)}}}),$$

$$STS^{-1} = (a_{i_{i_{l(1)}}+1} a_{i_{i_{l(2)}}+1} \cdots a_{i_{i_{l(n)}}+1})$$

et $$TST^{-1} = (a_{i_{l(1)}+1} a_{i_{l(2)}+1} \ldots a_{i_{l(n)}+1}),$$

chaque indice supérieur à n devant être réduit mod. n.

Or, des égalités (VI) il résulte que

$$a_{i_{i_{l(1)}}+1} = a_{i_{l(1)}+1},\ a_{i_{i_{l(2)}}+1} = a_{i_{l(2)}+1},\ \ldots,\ a_{i_{i_{l(n)}}+1} = a_{i_{l(n)}+1}.$$

On a donc bien $$STS^{-1} = TST^{-1}$$

et la condition énoncée est suffisante.

§ 2. Soit (VII) $$i_1, i_2, \ldots, i_n$$

une suite formée des nombres entiers $1, 2, \ldots, n$ pris dans un ordre déterminé *qui n'est pas l'ordre naturel*, et soit

(VIII) $$i_{i_1}+1 = i_2,\ i_{i_2}+1 = i_3,\ \ldots,\ i_{i_n}+1 = i_1$$

(les nombres supérieurs à n étant partout remplacés par leur reste mod. n).

Remarquons d'abord que (VII) $i_1, i_2, \ldots, i_n$ étant une permutation quelconque des nombres $1, 2, \ldots, n$, quel que soit le nombre entier i_j $(1 \leq j \leq n)$, si l'on forme la suite des nombres

(*) $$i_j,\ i_{i_j},\ i_{i_{i_j}},\ \ldots,\ \underbrace{i_{i_{\ldots_{i_j}}}}_{\Gamma_j},$$

qui tous appartiennent à (VII), Γ_j désignant le plus grand nombre entier, tel que la suite (*) soit composée de Γ_j termes distincts deux à deux, on a:

$$\underbrace{i_{i_{\ldots_{i_j}}}}_{\Gamma_j} = j.$$

Partons de l'élément i_1 de la suite (VII) et formons la suite

(1) $$a_1^1 = i_1,\ a_2^1 = i_{i_1},\ a_3^1 = i_{i_{i_1}},\ \ldots,\ a_{\alpha_1}^1 = \underbrace{i_{i_{\ldots_{i_1}}}}_{\alpha_1} = 1,$$

α_1 étant le plus petit entier, tel que $a_{\alpha_1}^1 = 1$.

Il est manifeste que $\alpha_1 \leq n$, puisque chaque élément de la suite (1) appartient à la suite (VII) et que ces éléments sont distincts deux à deux.

Montrons que l'élément i_2 n'appartient pas à la suite (1). En effet, supposons le contraire et soit t un entier compris au sens large entre 1 et α_1 et tel que $i_2 = a_t^1$.

On en déduit immédiatement que

$$i_{i_2} = a_{t+1}^1,\ i_{i_{i_2}} = a_{t+2}^1,\ \ldots,\ \underbrace{i_{i_{\cdots i_2}}}_{\alpha_1} = a_{t-1}^1,$$

les indices supérieurs à α_1 devant être réduits mod. α_1.

Ainsi la suite

$$(**) \qquad a_1^2 = i_2,\ a_2^2 = i_{i_2},\ \ldots,\ a_{\alpha_1}^2 = \underbrace{i_{i_{\cdots i_2}}}_{\alpha_1}$$

est une permutation circulaire de la suite (1). Elle se compose, par conséquent, de α_1 termes distincts et l'on a $a_{\alpha_1}^2 = 2$.

Des égalités (VIII) et des définitions précédentes, il résulte sans peine que $a_{2i}^1 + 1 = a_i^2 = a_{t+i-1}^1$ quel que soit $i = 1, 2, \ldots, n$, les indices *supérieurs* à α_1 devant être réduits mod. α_1, ce que nous écrirons $a_{2i\,(\text{mod. }\alpha_1)}^1 + 1 = a_i^2 = a_{t+i-1\,(\text{mod. }\alpha_1)}^1$.

Or, si $i = t - 1$, on a

$$a_{2i\,(\text{mod. }\alpha_1)}^1 = a_{2t-2\,(\text{mod. }\alpha_1)}^1,$$

$$a_{t+i-1\,(\text{mod. }\alpha_1)}^1 = a_{2t-2\,(\text{mod. }\alpha_1)}^1.$$

Donc

$$a_{2i-2\,(\text{mod. }\alpha_1)}^1 + 1 = a_{2t-2\,(\text{mod }\alpha_1)}^1,$$

ce qui est impossible. On est ainsi conduit à une contradiction. Par conséquent, l'élément i_2 n'appartient pas à la suite (1) et $\alpha_1 < n$.

Il en résulte sans peine que les suites (1) et

$$(2) \qquad a_1^2 = i_2,\ a_2^2 = i_{i_2},\ \ldots,\ a_{\alpha_2}^2 = \underbrace{i_{i_{\cdots i_2}}}_{\alpha_2} = 2,$$

où α_2 est le plus petit nombre entier, tel que $a_{\alpha_2}^2 = 2$, n'ont aucun élément commun.

Des relations $a_{2i\,(\text{mod. }\alpha_1)}^1 + 1 = a_i^2$ qui ont toujours lieu en vertu de (VIII), il ressort que si α_1 est pair, $\alpha_2 = \frac{\alpha_1}{2}$, et que si α_1 est impair, $\alpha_2 = \alpha_1$.

Montrons que $\alpha_2 = \alpha_1$.

Formons, pour tout nombre entier j compris au sens large entre 1 et n, la suite

$$(j) \qquad a_1^j = i_j,\ a_2^j = i_{i_j},\ \ldots,\ a_{\alpha_j}^j = \underbrace{i_{i_{\ldots_{i_j}}}}_{\alpha_j} = j,$$

α_j désignant le plus petit entier, tel que $a_{\alpha_j}^j = j$.

Des égalités (VIII) et de ces définitions, il résulte sans peine que

$$a^j_{2i \,(\mathrm{mod.}\ \alpha_j)} + 1 = a_i^{j+1 \,(\mathrm{mod.}\ n)} \qquad (i = 1, 2, \ldots, \alpha_j;\ j = 1, 2, \ldots, n).$$

On en déduit que, quel que soit $j = 1, 2, \ldots, n$, $\alpha_{j+1} = \frac{\alpha_j}{2}$, si α_j est pair, que $\alpha_{i+1} = \alpha_j$, si α_j est impair, $j+1$ devant être remplacé par 1, si $j = n$, et, d'autre part, que $\alpha_1 \geqq \alpha_2 \geqq \alpha_3 \geqq \ldots \geqq \alpha_n \geqq \alpha_1$. Donc $\alpha_1 = \alpha_2 = \ldots = \alpha_n = \alpha$ et ce nombre α est *impair*.

En outre, $\alpha > 1$. En effet, si $\alpha = 1$ il en résulte que $i_1 = 1$, $i_2 = 2, \ldots, i_n = n$, contrairement à notre hypothèse sur la suite (VII). Donc $\alpha \geqq 3$.

On vérifie aisément qu'à deux valeurs distinctes j_1 et j_2 de l'entier j $(1 \leqq j \leqq n)$ correspondent soit deux suites disjointes (j_1) et (j_2), soit deux suites (j_1) et (j_2) composées des mêmes éléments de (VII) et dont l'une est une permutation circulaire de l'autre. Donc n est un multiple de α. Soit $n = k\alpha$. Le nombre k est $\geqq 2$. Donc n ne peut pas être un nombre premier.

Je dis que les k premières suites (j), $j = 1, 2, \ldots, k$, contiennent tous les éléments de la suite (VII).

En effet, soit l le plus petit nombre entier, tel que la suite (l) soit une permutation circulaire d'une des suites précédentes, soit de la suite (t), $(t < l)$: $a_1^l = a_r^t$, $a_2^l = a_{r+1}^t$, $\ldots$, $a_n^l = a_{r-1}^t$. Alors, des égalités $a^l_{2i(\mathrm{mod.}\alpha)} + 1 = a_i^{l+1}$ et $a^t_{2i(\mathrm{mod.}\alpha)} + 1 = a_i^{t+1}$, il résulte que la suite $(l+1)$ est une permutation circulaire de la suite $(t+1)$; d'où on déduit de la même façon que la suite $(l+2)$ est une permutation circulaire de la suite $(t+2)$ et ainsi de suite, la suite (n) est une permutation circulaire de la suite $(t+n-l)$. Donc aucune suite (j), où $j \geqq l$, ne contient d'éléments de la suite (VII) qui n'appartiennent pas à une suite (j'), où $j' < l$. Comme, d'autre part, tout élément de la suite (VII) appartient à l'une des suites (j), par définition de ces suites, on doit nécessairement avoir $l = k+1$ et notre assertion est démontrée.

Ainsi, nous avons décomposé la suite (VII) en k suites distinctes

$$(1) \qquad a_1^1,\ a_2^1,\ \ldots,\ a_\alpha^1 = 1$$

$$(2) \qquad a_1^2,\ a_2^2,\ \ldots,\ a_\alpha^2 = 2$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$(k) \qquad a_1^k,\ a_2^k,\ \ldots,\ a_\alpha^k = k,$$

pour lesquelles on a

$$a^j_{2i\,(\mathrm{mod.}\,\alpha)} + 1 = a_i^{j+1} \quad (j = 1, 2, 3, \ldots, k;\ i = 1, 2, 3, \ldots, \alpha).$$

On en déduit successivement les égalités

$$a^1_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^2_i$$
$$a^2_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^1_{2^2 i\,(\mathrm{mod.}\,\alpha)}+2=a^3_i$$
$$a^3_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^1_{2^3 i\,(\mathrm{mod.}\,\alpha)}+3=a^4_i$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a^{k-1}_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^1_{2^{k-1} i\,(\mathrm{mod.}\,\alpha)}+k-1=a^k_i$$

Il ressort de ces égalités qu'on obtient, à l'ordre près, tous les éléments de la suite (j), $j=2, 3, \ldots, n$, en ajoutant $j-1$ à chaque terme de la suite (1).

Si donc la suite (1) contient un nombre μ, les suites (1), (2), ..., (k) n'ayant deux à deux aucun élément commun, (1) ne peut contenir aucun des nombres $\mu \pm j$ $(j=1, 2, \ldots, k-1)$.

Comme, d'autre part, tous les nombres de la suite (1) appartiennent à la suite des nombres $1, 2, \ldots, n$ et que la suite (1) contient le nombre 1, on voit qu'à l'ordre près, les termes de la suite (1) doivent nécessairement prendre les valeurs $1, 1+k, 1+2k, \ldots, 1+(\alpha-1)k$.

La suite $(k+1)$ $\quad a_1^{k+1}, a_2^{k+1}, \ldots, a_\alpha^{k+1}$

est une permutation circulaire de la suite (1). En effet, nous avons vu que cette suite est une permutation circulaire d'une suite

(j_1) $\qquad a_1^{j_1}, a_2^{j_1}, \ldots, a_\alpha^{j_1} \qquad (1 \leq j_1 \leq k)$.

Si $j_1 > 1$, toute suite (j) $a_1^j, a_2^j, \ldots, a_\alpha^j$, où $j > k$, et en particulier la suite (n), est une permutation circulaire d'une des suites $(j_1), (j_1+1), \ldots, (k)$. Il en sera donc de même de la suite (1), en vertu des égalités $a^n_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^1_i$, $i=1, 2, \ldots, \alpha$, ce qui est impossible. On a donc bien $j_1=1$.

Or, des égalités

$$a^k_{2i\,(\mathrm{mod.}\,\alpha)}+1=a^1_{2^k i\,(\mathrm{mod.}\,\alpha)}+k=a^{k+1}_i \qquad (i=1, 2, \ldots, a)$$

et du fait que la suite $(k+1)$ est une permutation circulaire de la suite (1), il résulte qu'il doit exister un nombre entier r, compris au sens large entre 1 et α et tel que

$$\text{(IX)} \quad \left\{ \begin{array}{l} a^1_{2^k}+k=a^1_{r+1} \\ a^1_{2\cdot 2^k}+k=a^1_{r+2} \\ \ldots\ldots\ldots\ldots \\ a^1_{i\cdot 2^k}+k=a^1_{r+i} \\ \ldots\ldots\ldots\ldots \\ a^1_{\alpha\cdot 2^k}+k=a^1_r, \end{array} \right. \qquad (\mathrm{mod.}\ n)$$

tous les indices supérieurs à α devant être réduits mod. α. Comme les termes de la suite (1) prennent, à l'ordre près, les valeurs $1, 1+k, 1+2k, \ldots, 1+(\alpha-1)k$, nous pouvons poser

$$(X)\quad \begin{cases} a_1^1 = 1 + \varrho_1 k \\ a_2^1 = 1 + \varrho_2 k \\ \cdots\cdots\cdots\cdots \\ a_i^1 = 1 + \varrho_i k \\ \cdots\cdots\cdots\cdots \\ a_\alpha^1 = 1 + \varrho_\alpha k \end{cases} \qquad (\text{mod. } n)$$

où $\varrho_1, \varrho_2, \ldots, \varrho_{\alpha-1}$ sont, à l'ordre près, les nombres 1, 2, ..., $\alpha - 1$ et $\varrho_\alpha = \alpha$.

Soit $2^k \equiv t \pmod{\alpha}$, $0 \leq t < \alpha$.

Comme α est un nombre impair, on a $t \geq 1$ et les nombres entiers t et α sont premiers entre eux.

En tenant compte de (X), on obtient de (IX) les égalités

$$(XI)\quad \begin{cases} \varrho_t + 1 = \varrho_{r+1} \\ \varrho_{2t} + 1 = \varrho_{r+2} \\ \cdots\cdots\cdots\cdots \\ \varrho_{it} + 1 = \varrho_{r+i} \\ \cdots\cdots\cdots\cdots\cdots \\ \varrho_{\alpha t} + 1 = 1 = \varrho_r, \end{cases}$$

les nombres supérieurs à α devant être réduits mod. α.

Deux cas peuvent se présenter :

a) $t = 1$.

Il résulte alors de (XI) que

$$\begin{cases} \varrho_1 + 1 = \varrho_{r+1} \\ \varrho_2 + 1 = \varrho_{r+2} \\ \cdots\cdots\cdots\cdots \\ \varrho_i + 1 = \varrho_{r+i} \\ \cdots\cdots\cdots\cdots \\ \varrho_\alpha + 1 = 1 = \varrho_r \end{cases} \qquad (\text{mod. } \alpha)$$

On en déduit successivement

$$(XII)\quad \begin{cases} \varrho_r = 1 \\ \varrho_{2r} = \varrho_r + 1 = 2 \\ \cdots\cdots\cdots\cdots\cdots \\ \varrho_{ir} = \varrho_{(i-1)r} + 1 = i \\ \cdots\cdots\cdots\cdots\cdots \\ \varrho_{\alpha r} = \varrho_\alpha = \alpha, \end{cases}$$

les indices supérieurs à α étant toujours réduits mod. α.

Comme la suite des nombres ϱ_r, ϱ_{2r}, ..., $\varrho_{\alpha r}$, où les indices doivent être réduits mod. α s'ils sont supérieurs à α, est composée de α termes distincts 1, 2, ..., α, il doit en être de même de la suite des nombres r, $2r$, $3r$, ..., αr, réduits mod. α, s'ils sont supérieurs à α. Par conséquent, r et α doivent nécessairement être premiers entre eux.

D'autre part, de (XII) on déduit (XIII)

$$\begin{cases} \varrho_1 = \varrho_{\varrho_1 r} \\ \varrho_2 = \varrho_{\varrho_2 r} \\ \cdots\cdots\cdots \\ \varrho_i = \varrho_{\varrho_i r} \\ \cdots\cdots\cdots \\ \varrho_\alpha = \varrho_{\varrho_\alpha r} \end{cases}$$

les indices $> \alpha$ devant être réduits mod. α.

Il en résulte immédiatement que

$$\begin{cases} \varrho_1 r \equiv 1 \pmod{\alpha} \\ \varrho_2 r \equiv 2 \pmod{\alpha} \\ \cdots\cdots\cdots\cdots\cdots \\ \varrho_i r \equiv i \pmod{\alpha} \\ \cdots\cdots\cdots\cdots\cdots \\ \varrho_\alpha r \equiv o \pmod{\alpha} \end{cases}$$

d'où on déduit les congruences

$$r(\varrho_2 - \varrho_1) \equiv r(\varrho_3 - \varrho_2) \equiv \ldots \equiv r(\varrho_i - \varrho_{i-1}) \equiv \ldots \equiv r(\varrho_\alpha - \varrho_{\alpha-1}) \equiv 1 \pmod{\alpha}.$$

Comme r et α sont premiers entre eux et comme $1 \leq \varrho_i - \varrho_{i-1} < \alpha$ quel que soit $i = 2, 3, \ldots, \alpha$, on déduit de ces congruences les égalités

(XIV) $$\varrho_2 - \varrho_1 = \varrho_3 - \varrho_2 = \ldots = \varrho_i - \varrho_{i-1} = \ldots = \varrho_\alpha - \varrho_{\alpha-1} = A,$$

A désignant la valeur commune de toutes ces différences.

Montrons que $A = \varrho_1$.

En effet, des égalités (X) on déduit, en tenant compte de (XIV),

$$a_1^1 = 1 + \varrho_1 k,$$
$$a_2^1 = 1 + \varrho_2 k = 1 + (\varrho_1 + \varrho_2 - \varrho_1) k = 1 + (\varrho_1 + A) k,$$

et en général, quel que soit le nombre entier $i > 1$ et $\leq \alpha$, si l'on suppose que

$$a_{i-1}^1 = 1 + \varrho_{i-1} k = 1 + [\varrho_1 + (i-2) A] k,$$

on a $$a_i^1 = 1 + \varrho_i k = 1 + (\varrho_{i-1} + \varrho_i - \varrho_{i-1}) k = 1 + [\varrho_1 + (i-1) A] k.$$

En particulier, pour $i = \alpha$, on a

$$a_\alpha^1 = 1 = 1 + [\varrho_1 + (\alpha - 1) A] k \pmod{n}.$$

Donc $[\varrho_1+(\alpha-1)A]k\equiv 0 \pmod{n}$.

Or, $n=k\alpha$.

On a donc (XV) $\varrho_1+(\alpha-1)A\equiv 0 \pmod{\alpha}$.

Or, $1\leq\varrho_1\leq\alpha-1$ et $1\leq A\leq\alpha-1$.

La congruence (XV) n'est donc possible que si $\varrho_1=A$, c. q. f. d. Par conséquent, $\varrho_i\equiv i\varrho_1 \pmod{\alpha}$, $(i=1, 2, \ldots, \alpha)$, et comme $\varrho_r=1$, on doit avoir $r\varrho_1\equiv 1 \pmod{\alpha}$. Il résulte de cette dernière congruence que ϱ_1 est premier avec α.

Inversement on établit sans peine, en tenant compte des considérations qui précèdent, que pour tout nombre entier n de la forme $n=k\alpha$, où k est un entier ≥ 2, α est un entier impair ≥ 3 et $2^k\equiv 1 \pmod{\alpha}$, il existe des suites de la forme (VII) qui satisfont aux égalités (VIII). Il suffit de prendre à cet effet pour ϱ_1 un nombre entier quelconque compris au sens large entre 1 et $\alpha-1$ et premier avec α, puis, les notations étant les mêmes que ci-dessus, de poser

$$a_i^1=1+i\varrho_1 k,$$
$$a_i^j=a_{i2^{j-1}\,(\text{mod. }\alpha)}^1+j-1$$

$(i=1, 2, \ldots, \alpha;\ j=2, 3, \ldots, k)$, tous les nombres a_i^1, a_i^j supérieurs à n devant être réduits mod. n.

b) Soit à présent $t>1$.

Partons des égalités (XI).

On a $\varrho_\alpha=\alpha=\varrho_{r+\alpha-r}=\varrho_{(\alpha-r)t}+1$.

Donc $\varrho_{\alpha t-tr}=\alpha-1$.

Or, $\varrho_{\alpha t-tr}=\varrho_{r+\alpha t-(t+1)r}=\varrho_{[\alpha t-(t+1)r]t}+1$, d'où on conclut que $\varrho_{\alpha t^2-(t^2+t)r}=\alpha-2$.

D'une façon générale, quel que soit le nombre entier $i>1$ et $\leq\alpha-1$, si nous supposons que $\varrho_{\alpha t^{i-1}-(t^{i-1}+t^{i-2}\ldots+t)r}=\alpha-i+1$, on a :

$$\varrho_{\alpha t^{i-1}-(t^{i-1}+t^{i-2}+\ldots+t)r}=\varrho_{r+\alpha t^{i-1}-(t^{i-1}+t^{i-2}+\ldots+t+1)r}$$
$$=\varrho_{\alpha t^i-(t^i+t^{i-1}+\ldots+t)r}+1=\alpha-i+1.$$

D'où l'on déduit (XVI) $\varrho_{\alpha t^i-(t^i+t^{i-1}+\ldots+t)r}=\alpha-i.$

En particulier, pour $i=\alpha-1$, on a $\varrho_{\alpha t^{\alpha-1}-(t^{\alpha-1}+t^{\alpha-2}+\ldots+t)r}=1=\varrho_r$.

Donc $\alpha t^{\alpha-1}-(t^{\alpha-1}+t^{\alpha-2}+\ldots+t)r\equiv r \pmod{\alpha}$,

ou encore $$r\frac{t^\alpha-1}{t-1}\equiv 0 \pmod{\alpha}$$

Donc aussi (XVII) $r(t^\alpha-1)\equiv 0 \pmod{\alpha}$.

Montrons que α ne saurait être un nombre premier. En effet, supposons le contraire. Alors comme t n'est pas un multiple de α,

on a en vertu du petit théorème de Fermat, $t^{\alpha-1}-1\equiv 0$ (mod. α), donc aussi $t^{\alpha}-t\equiv 0$ (mod. α) et de (XVII) on déduit : $t^{\alpha}-1\equiv 0$ (mod. α).

En soustrayant membre à membre ces deux congruences, on trouve $t-1\equiv 0$ (mod. α).

Or, $1\leq t-1<\alpha$. La dernière congruence ne peut donc pas avoir lieu, ce qui prouve bien que α ne saurait être un nombre premier.

La suite ϱ_{α}, $\varrho_{\alpha t-tr}$, $\varrho_{\alpha t^2-(t^2+t)r}$, $\cdots$, $\varrho_{\alpha t^{\alpha-1}-(t^{\alpha-1}+t^{\alpha-2}+\ldots+t)r}$, où les indices supérieurs à α doivent être réduits mod. α, étant composée de α nombres distincts 1, 2, ..., α, il doit en être de même de la suite des indices α, $\alpha t-tr$, $\alpha t^2-(t^2+t)r$, ..., $\alpha t^{\alpha-1}-(t^{\alpha-1}+t^{\alpha-2}+\ldots+t)r$, ces indices devant être réduits mod. α s'ils sont supérieurs à α.

Donc la suite des nombres t, t^2+t, ..., $t^{\alpha-1}+t^{\alpha-2}+\ldots+t$, réduits selon le module α, doit contenir $\alpha-1$ nombres entiers distincts, à savoir 1, 2, ..., $\alpha-1$.

Il en découle que r et α sont premiers entre eux. En effet, supposons le contraire et soit δ un nombre entier >1 qui est diviseur aussi bien de r que de α, avec $\alpha=\alpha_1\delta$, $r=r_1\delta$.

La suite des nombres t, t^2+t, ..., $t^{\alpha-1}+t^{\alpha-2}+\ldots+t$, réduits mod. α, comprenant tous les nombre 1, 2, ..., $\alpha-1$, il existera un terme de cette suite qui est égal à α_1. Soit i', $1\leq i'\leq\alpha-1$, le nombre entier, tel que $t^{i'}+t^{i'-1}+\ldots+t\equiv\alpha_1$ (mod. α).

On a alors $(t^{i'}+t^{i'-1}+\ldots t)r\equiv\alpha_1\delta r_1\equiv o$ (mod. α).

Donc $\alpha t^{i'}-(t^{i'}+t^{i'-1}+\ldots+t)r\equiv o$ (mod. α).

Or cela est impossible puisque la suite des nombres

$$\alpha,\ \alpha t-tr,\ \ldots,\ \alpha t^{\alpha-1}-(t^{\alpha-1}+t^{\alpha-2}+\ldots+t)r,$$

réduits mod. α s'ils sont supérieurs à α, à laquelle appartient le nombre $\alpha t^{i'}-(t^{i'}+t^{i'-1}+\ldots+t)r$ et dont il n'est pas le premier terme, est composée de α nombres distincts 1, 2, ..., α et que le premier terme de cette suite est déjà égal à α.

Ainsi r et α sont bien premiers entre eux.

De (XVII) on déduit donc (XVIII) $t^{\alpha}-1\equiv 0$ (mod. α) ou, en tenant compte du fait que $2^k\equiv t$ (mod. α)

(XVIII′) $2^{k\alpha}-1\equiv 0$ (mod. α).

Désignons par β le plus petit nombre entier, tel que

(XIX) $2^{\beta}\equiv 1$ (mod. α).

On a $\beta<\alpha$.

De (XVIII′) et (XIX), il résulte (XX) $k\alpha=\mu\beta$, où μ est un nombre entier ≥ 1.

Soit $D(\alpha,\beta)=\vartheta$ le plus grand commun diviseur de α et β.

Si $\vartheta=1$, en vertu de (XX), k doit être un multiple de β.

Soit $k=k'\beta$. Mais alors $2^k\equiv 1 \pmod{\alpha}$, ce qui est contraire à notre hypothèse que $t>1$. On ne saurait donc avoir $\vartheta=1$. Par conséquent, $\vartheta>1$.

D'autre part, comme $\beta<\alpha$, on a $\vartheta<\alpha$.

Soit $\alpha=\alpha_1\vartheta$; $\beta=\beta_1\vartheta$, $(\alpha_1>1,\ \beta_1\geqq 1)$.

Comme α est un nombre impair, il en est de même de ϑ et de α_1.

On déduit de (XX): $k\alpha=k\alpha_1\vartheta=\mu\beta=\mu\beta_1\vartheta$, d'où il résulte que $k\alpha_1=\mu\beta_1$.

Comme $D(\alpha_1,\beta_1)=1$, on doit avoir $k=k_1\beta_1$, où k_1 est un nombre entier $\geqq 1$. Donc dans ce cas, le nombre n d'éléments de la suite (VII) qui satisfait aux égalités (VIII) est de la forme

$$n=k\alpha=k_1\beta_1\alpha_1\vartheta=\underline{k_1\beta\alpha_1}.$$

De la congruence (XIX) il résulte, comme $\alpha=\alpha_1\vartheta$: $2^\beta\equiv 1 \pmod{\alpha_1}$, et, quel que soit le nombre entier ν, on a également les congruences $2^{\nu\beta}\equiv 1 \pmod{\alpha}$ et $2^{\nu\beta}\equiv 1 \pmod{\alpha_1}$.

En particulier, pour $\nu=k_1$, on a aussi $2^{k_1\beta}\equiv 1 \pmod{\alpha_1}$.

Nous en concluons que quelle que soit la suite (VII) qui satisfait aux égalités (VIII), le nombre n d'éléments de cette suite est un produit de deux nombres entiers n_1 et n_2, dont le premier est impair $\geqq 3$, le second est $\geqq 2$, et qui satisfont à la congruence $2^{n_2}\equiv 1 \pmod{n_1}$.

Si l'on se borne à considérer les nombres entiers n compris au sens large entre 1 et 342, on vérifie aisément que pour $n=6$, 12, 18, 20, 21, 24, 30, 36, 40, 42, 48, 54, 60, 63, 66, 72, 78, 80, 84, 90, 96, 100, 102, 105, 108, 110, 114, 120, 126, 132, 136, 138, 140, 144, 147, 150, 156, 160, 162, 168, 174, 180, 186, 189, 192, 198, 200, 204, 210, 216, 220, 222, 228, 231, 234, 240, 246, 252, 258, 260, 264, 270, 272, 273, 276, 280, 282, 288, 294, 300, 306, 312, 315, 318, 320, 324, 330, 336, 340, 342, il existe des suites de la forme (VII) qui satisfont aux conditions (VIII) et qu'il n'en existe aucune pour toute autre valeur de n comprise dans le domaine envisagé.

Voici quelques exemples de suites de la forme (VII) qui satisfont aux égalités (VIII):

a) 3, 6, 5, 2, 1, 4
b) 5, 4, 1, 6, 3, 2
c) 3, 12, 11, 8, 1, 4, 9, 18, 17, 14, 7, 10, 15, 6, 5, 2, 13, 16
d) 17, 4, 13, 12, 9, 2, 5, 10, 1, 18, 15, 8, 11, 16, 7, 6, 3, 14
e) 15, 18, 5, 14, 13, 10, 3, 6, 11, 2, 1, 16, 9, 12, 17, 8, 7, 4
f) 11, 10, 7, 18, 3, 8, 17, 16, 13, 6, 9, 14, 5, 4, 1, 12, 15, 2
g) 9, 6, 17, 2, 7, 16, 15, 12, 5, 8, 13, 4, 3, 18, 11, 14, 1, 10
h) 5, 16, 1, 6, 15, 14, 11, 4, 7, 12, 3, 2, 17, 10, 13, 18, 9, 8
i) 7, 14, 9, 16, 11, 18, 13, 2, 15, 4, 17, 6, 1, 8, 3, 10, 5, 12
j) 13, 8, 15, 10, 17, 12, 1, 14, 3, 16, 5, 18, 7, 2, 9, 4, 11, 6

Pour les suites a) et b), on a : $n=6$, $k=2$, $\alpha=3$, $2^k \equiv 1 \pmod{\alpha}$.

Pour les suites c), d), e), f), g), h) on a : $n=18$, $k=2$, $\alpha=9$, $2^k \equiv 4 \pmod{\alpha}$.

Pour les suites i) et j), on a : $n=18$, $k=6$, $\alpha=3$, $2^k \equiv 1 \pmod{\alpha}$.

Ce sont là tous les cas possibles pour $n=6$ et $n=18$.

Chapitre II

Soient à présent S et T deux substitutions de second ordre portant sur les mêmes n éléments chacune.

Montrons que la condition nécessaire et suffisante pour que ces deux substitutions soient des transformées réciproques est que n soit un nombre de la forme

$$n = k_1 + 2k_2 + 3k_3 + 6k_4,$$

où k_1, k_2, k_3, k_4 sont des nombres entiers non négatifs, l'un au moins des nombres k_3, k_4 étant $\neq O$, si $S \neq T$, et que les n éléments de $S(T)$ forment k_1 groupes d'un élément chacun, cet élément constituant un cycle de premier ordre commun à S et à T, k_2 groupes de deux éléments chacun, ces deux éléments formant une transposition commune à S et à T, k_3 groupes de trois éléments chacun, ces trois éléments formant un cycle de premier ordre et une transposition aussi bien dans S que dans T, mais ces deux cycles étant distincts pour les deux substitutions, et k_4 groupes de six éléments chacun, ces six éléments formant trois transpositions aussi bien dans S que dans T et dont aucune n'est commune à ces deux substitutions.

a) *La condition est nécessaire.*

Soient S et T deux substitutions de second ordre et soit

$$(1) \qquad STS^{-1} = TST^{-1}$$

Ces deux substitutions sont semblables et ne peuvent contenir que des cycles de premier et de second ordre.

Soit (a_1) un cycle quelconque de premier ordre de S.

Deux cas peuvent se présenter :

Ou bien le cycle (a_1) figure aussi dans T. Il fait donc partie de $STS^{-1} = TST^{-1}$.

Ou bien T possède une transposition, dont l'un des éléments est a_1.

Soit $(a_1 a_2)$ cette transposition. Dans ce cas, TST^{-1} contient le cycle (a_2). Mais alors, en vertu de l'égalité (1), il doit exister dans T un cycle (a_3) de premier ordre, tel que $a_3 \neq a_1$ et que S contienne la transposition $(a_3 a_2)$. Ainsi, les trois éléments a_1, a_2, a_3 forment

un cycle de premier ordre et une transposition aussi bien dans S que dans T et ces deux cycles sont distincts pour les deux substitutions.

Soit, à présent $(a_1 a_2)$ une transposition quelconque de S.

Les cas suivants pourraient avoir lieu :

1) T contient également la transposition $(a_1 a_2)$. Alors $(a_1 a_2)$ appartient aussi à $STS^{-1} = TST^{-1}$.

2) T contient les cycles (a_1) et (a_2). Alors la transposition $(a_1 a_2)$ appartient à TST^{-1}. Elle doit donc aussi appartenir à STS^{-1} en vertu de l'égalité (1). Or, c'est impossible, car il devrait exister dans T une transposition $(a_3 a_4)$, $a_3 \neq a_1, a_2$; $a_4 \neq a_1, a_2$, et dans S deux transpositions $(a_3 a_1)$ et $(a_4 a_2)$, ce qui ne saurait avoir lieu puisque S contient la transposition $(a_1 a_2)$ et que cette substitution est de second ordre. Le cas 2) ne peut donc pas se présenter.

3) T contient le cycle (a_1) $[(a_2)]$ et une transposition $(a_2 a_3)$ $[(a_1 a_3)]$. Alors TST^{-1} contient la transposition $(a_1 a_3)$ $[(a_3 a_2)]$ qui doit également appartenir à STS^{-1} en vertu de l'égalité (1). Or, S transforme a_2 en a_1 [a_1 en a_2]. Donc T doit contenir une transposition $(a_2 a_4)$ $[(a_4 a_1)]$ qui, transformée par S, donne $(a_1 a_3)$ $[(a_3 a_2)]$ et, comme T contient déjà la transposition $(a_2 a_3)$ $[(a_1 a_3)]$, on doit avoir $a_4 = a_3$. Donc S doit contenir le cycle (a_3).

Ainsi donc les éléments a_1, a_2, a_3 forment un cycle de premier ordre et une transposition aussi bien dans S que dans T et ces deux cycles sont distincts pour les deux substitutions.

4) T contient deux transpositions $(a_1 a_3)$ $(a_2 a_4)$, les éléments a_1, a_2, a_3, a_4 étant distincts deux à deux.

Alors, $(a_1 a_2)$ appartenant à S, la transposition $(a_3 a_4)$ appartient à TST^{-1}. Elle doit donc aussi appartenir à STS^{-1}, d'où il découle que T doit contenir une certaine transposition $(a_5 a_6)$, telle que S contienne les transpositions $(a_5 a_3)$ et $(a_6 a_4)$. Comme S contient déjà la transposition $(a_1 a_2)$, les éléments a_5, a_6 doivent nécessairement être distincts de a_1, a_2, a_3, a_4. Il existe donc dans ce cas six éléments a_1, a_2, a_3, a_4, a_5, a_6 qui forment trois transpositions aussi bien dans S que dans T, aucune de ces transpositions n'étant commune à S et à T.

Il résulte sans peine de ces considérations que la condition énoncée est bien nécessaire pour que les substitutions S et T soient des transformées réciproques.

b) *La condition est suffisante.* Supposons qu'elle est satisfaite. Chaque cycle de premier ou de second ordre commun à S et à T appartient évidemment aussi bien à STS^{-1} qu'à TST^{-1}.

Soit a_1, a_2, a_3 un groupe de trois éléments formant dans S les cycles (a_1) $(a_2 a_3)$ et dans T les cycles $(a_1 a_2)$ (a_3) $[(a_1 a_3)(a_2)]$. En effectuant sur les éléments des cycles (a_1) $(a_2 a_3)$ la substitution T, on obtient les cycles (a_2) $(a_1 a_3)$ $[(a_3)(a_2 a_1)]$ et en effectuant sur les éléments des cycles $(a_1 a_2)(a_3)[(a_1 a_3)(a_2)]$ la substitution S, on trouve

les cycles $(a_2)(a_1a_3)[(a_1a_2)(a_3)]$, identiques à ceux que nous avons obtenus précédemment.

Soit, à présent, a_1, a_2, a_3, a_4, a_5, a_6 un groupe de six éléments formant dans S les transpositions $(a_1a_2)(a_3a_4)(a_5a_6)$ et dans T un quelconque des huit groupes de transpositions

$$\begin{array}{l}(a_1a_3)(a_2a_5)(a_4a_6)\\(a_1a_3\ (a_2a_6)(a_4a_5)\\(a_1a_4)(a_2a_5)(a_3a_6)\\(a_1a_4)(a_2a_6)(a_3a_5)\\(a_1a_5)(a_2a_3)(a_4a_6)\\(a_1a_5)(a_2a_4)(a_3a_6)\\(a_1a_6)(a_2a_3)(a_4a_5)\\(a_1a_6)(a_2a_4)(a_3a_5),\end{array}$$

par exemple $(a_1a_4)(a_2a_6)(a_3a_5)$.

Si l'on effectue sur les éléments des trois transpositions en question de S la substitution T, on obtient les transpositions (a_4a_6) $(a_5a_1)(a_3a_2)$ et si on effectue sur les éléments des transpositions correspondantes de T la substitution S, on obtient les transpositions $(a_2a_3)(a_1a_5)(a_4a_6)$ que l'on peut aussi écrire $(a_4a_6)(a_5a_1)(a_3a_2)$.

Si nous posons $S_1=(a_1a_2)(a_3a_4)(a_5a_6)$ et $T_1=(a_1a_4)(a_2a_6)(a_3a_5)$, on a donc $T_1S_1T_1^{-1}=S_1T_1S_1^{-1}$. On vérifie aisément que le résultat est le même si les éléments a_1, a_2, a_3, a_4, a_5, a_6 forment dans T l'un quelconque des sept autres systèmes signalés de transpositions.

Si donc la condition énoncée est satisfaite, on a bien

$$STS^{-1}=TST^{-1}, \tag{1}$$

et la condition est suffisante, c. q. f. d.

Passons maintenant aux substitutions de troisième ordre.

Soit C un cycle quelconque de troisième ordre d'une telle substitution et soit a_λ^C un élément arbitraire de ce cycle, l'indice λ pouvant prendre l'une des valeurs 1, 2, 3. Convenons de désigner par $a_{\lambda-1}^C$ l'élément du cycle C qui précède a_λ^C et par $a_{\lambda+1}^C$ l'élément du cycle C qui suit a_λ^C, les indices $\lambda-1$ et $\lambda+1$ devant être au besoin réduits selon le module 3, de façon à prendre toujours l'une des valeurs 1, 2, 3.

Par un raisonnement analogue à celui effectué pour les substitutions de second ordre, on établit sans peine que la condition nécessaire et suffisante pour que deux substitutions S et T de troisième ordre soient des transformées réciproques est que le nombre n des éléments de ces substitutions soit de la forme

$$n=k_1+3k_2+7k_3+21k_4,$$

où k_1, k_2, k_3, k_4 sont des nombres entiers non négatifs, l'un au moins des nombres k_3, k_4 étant $\neq 0$, si $S\neq T$, et que les éléments

de $S(T)$ forment k_1 groupes d'un élément chacun, cet élément constituant un cycle de premier ordre commun à S et à T, k_2 groupes de trois éléments chacun, ces trois éléments formant un cycle de troisième ordre commun à S et à T, k_3 groupes de sept éléments chacun, ces sept éléments formant deux cycles de troisième ordre et un cycle de premier ordre aussi bien dans S que dans T et tels que si l'on désigne par a_i^{I} un élément arbitraire de l'un de ces deux cycles de troisième ordre de S, par a_j^{II} un élément arbitraire du second de ces cycles de troisième ordre de S et par a_1^{III} l'élément du cycle envisagé de premier ordre de S, il existe deux éléments a_i^{I}, a_j^{II}, tels que T contient les cycles (a_i^{I}) $(a_{i+1}^{\mathrm{I}} a_j^{\mathrm{II}} a_1^{\mathrm{III}})$ $(a_{i-1}^{\mathrm{I}} a_{j-1}^{\mathrm{II}} a_{j+1}^{\mathrm{II}})$, les cycles correspondants de S pouvant être écrits sous la forme (a_1^{III}) $(a_{i-1}^{\mathrm{I}} a_i^{\mathrm{I}} a_{i+1}^{\mathrm{I}})$ $(a_{j-1}^{\mathrm{II}} a_j^{\mathrm{II}} a_{j+1}^{\mathrm{II}})$, enfin k_4 groupes de *21* éléments chacun, ces *21* éléments constituant sept cycles de troisième ordre aussi bien dans S que dans T et tels que si l'on numérote les cycles en question de S, pris dans un ordre arbitraire, au moyen des nombres I, II, III, IV, V, VI, VII et si l'on désigne par

a_i^{I}	un élément	arbitraire	du cycle	I
a_j^{II}	»	»	»	II
a_l^{III}	»	»	»	III
a_m^{IV}	»	»	»	IV
a_r^{V}	»	»	»	V
a_s^{VI}	»	»	»	VI
a_t^{VII}	»	»	»	VII

il existe sept éléments a_i^{I}, a_j^{II}, a_l^{III}, a_m^{IV}, a_r^{V}, a_s^{VI}, a_t^{VII}, tels que T contient les cycles $(a_i^{\mathrm{I}} a_j^{\mathrm{II}} a_l^{\mathrm{III}})$ $(a_{i+1}^{\mathrm{I}} a_m^{\mathrm{IV}} a_r^{\mathrm{V}})$ $(a_{i-1}^{\mathrm{I}} a_s^{\mathrm{VI}} a_t^{\mathrm{VII}})$ $(a_{j-1}^{\mathrm{II}} a_{m-1}^{\mathrm{IV}} a_{s-1}^{\mathrm{VI}})$ $(a_{j+1}^{\mathrm{II}} a_{t-1}^{\mathrm{VII}} a_{r+1}^{\mathrm{V}})$ $(a_{m+1}^{\mathrm{VI}} a_{l-1}^{\mathrm{III}} a_{t+1}^{\mathrm{VII}})$ $(a_{s+1}^{\mathrm{VI}} a_{r-1}^{\mathrm{V}} a_{l+1}^{\mathrm{III}})$, les cycles correspondants de S pouvant être écrits sous la forme $(a_{i-1}^{\mathrm{I}} a_i^{\mathrm{I}} a_{i+1}^{\mathrm{I}})$ $(a_{j-1}^{\mathrm{II}} a_j^{\mathrm{II}} a_{j+1}^{\mathrm{II}})$ $(a_{l-1}^{\mathrm{III}} a_l^{\mathrm{III}} a_{l+1}^{\mathrm{III}})$ $(a_{m-1}^{\mathrm{IV}} a_m^{\mathrm{IV}} a_{m+1}^{\mathrm{IV}})$ $(a_{r-1}^{\mathrm{V}} a_r^{\mathrm{V}} a_{r+1}^{\mathrm{V}})$ $(a_{s-1}^{\mathrm{VI}} a_s^{\mathrm{VI}} a_{s+1}^{\mathrm{VI}})$ $(a_{t-1}^{\mathrm{VII}} a_t^{\mathrm{VII}} a_{t+1}^{\mathrm{VII}})$.

Manuscrit reçu le 28 février 1936.
Dernières épreuves corrigées le 8 octobre 1936.