Zeitschrift: L'Enseignement Mathématique

Band: 38 (1939-1940)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: QUELQUES PROPOSITIONS CONCERNANT LES BASES DU GROUPE SYMÉTRIQUE ET DU GROUPE ALTERNÉ

Autor: Piccard, Sophie

DOI: https://doi.org/10.5169/seals-515788

QUELQUES PROPOSITIONS CONCERNANT LES BASES DU GROUPE SYMÉTRIQUE ET DU GROUPE ALTERNÉ

PAR

Sophie PICCARD (Neuchâtel).

Quel que soit le nombre entier $n \geqslant 3$ ($\geqslant 4$), on nomme *base* du groupe symétrique $\mathfrak{S}_n$ d'ordre $n!$ (du groupe alterné $\mathfrak{A}_n$ d'ordre $n!/2$) tout couple de substitutions du groupe envisagé qui permettent de l'engendrer, par composition.

Désignons par $1, 2, \ldots, n$ les éléments d'une substitution de $\mathfrak{S}_n$ ($\mathfrak{A}_n$). Nous disons que deux substitutions S et T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) sont *connexes* s'il n'existe aucun vrai sous-ensemble E_1 de l'ensemble $E = \{1, 2, \ldots, n\}$ qui soit transformé en lui-même aussi bien par la substitution S que par la substitution T.

Nous disons que deux substitutions connexes S et T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) sont *imprimitives* s'il existe une décomposition de l'ensemble E en un nombre $\geqslant 2$ de sous-ensembles disjoints deux à deux, comprenant chacun le même nombre > 1 d'éléments, et qui sont transformés les uns dans les autres aussi bien par la substitution S que par la substitution T. Dans le cas contraire, nous disons que les substitutions S, T sont primitives.

Une condition nécessaire pour que deux substitutions S, T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) puissent constituer une base de ce groupe, c'est qu'elles soient primitives.

Quels que soient le nombre entier $n > 1$ ainsi que les deux nombres a, b de la suite $1, 2, \ldots, n$, nous désignons par le

symbole $\overline{ab}$ le plus petit nombre entier positif vérifiant la congruence $a + \overline{ab} \equiv b \pmod{n}$.

Nous avons établi ailleurs les lemmes et propositions suivants:

Lemme 1. — Quels que soient le nombre entier $n > 2$ et les r $(2 \leqslant r \leqslant n)$ nombres $a_1, a_2, \ldots, a_r$ de la suite $1, 2, \ldots, n$, vérifiant l'égalité $D(\overline{a_1 a_2}, \overline{a_1 a_3}, \ldots, \overline{a_1 a_r}, n) = 1$, [1] en composant la substitution $S = (1\ 2 \ldots n)$ avec les transpositions $(a_1 a_2), (a_1 a_3), \ldots, (a_1 a_r)$, on obtient le groupe $\mathfrak{S}_n$.

Lemme 2. — Quels que soient le nombre pair (impair) $n > 3$ et les r $(3 \leqslant r \leqslant n)$ nombres $a_1, a_2, \ldots, a_r$ de la suite $1, 2, \ldots, n$, vérifiant l'égalité $D(\overline{a_1 a_2}, \overline{a_1 a_3}, \ldots, \overline{a_1 a_r}, n) = 1$, en composant la substitution $S = (1\ 2 \ldots n)$ avec les substitutions $(a_1 a_2 a_3), (a_1 a_2 a_4), \ldots, (a_1 a_2 a_r)$, on obtient le groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$.

Proposition 1. — Quels que soient les nombres entiers $k > 1$, i $(1 \leqslant i \leqslant k)$, $n > i$, les deux substitutions $S = (1\ 2 \ldots k)$, $T = (i\ i+1 \ldots n)$, si elles sont distinctes, engendrent le groupe $\mathfrak{S}_{\max.(k,n)}$, lorsque l'un au moins des deux nombres k, $n - i + 1$ est pair, ou le groupe $\mathfrak{A}_{\max.(k,n)}$, lorsque ces deux nombres sont impairs.

Proposition 2. — Quels que soient le nombre entier $n > 2$ et les deux nombres a, b de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (a\ b)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que $D(\overline{ab}, n) = 1$.

Proposition 3. — Quels que soient le nombre pair (impair) $n \geqslant 4$ et les trois nombres a, b, c de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (a\ b\ c)$ constituent une base du groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$, c'est que $D(\overline{ab}, \overline{ac}, n) = 1$.

Proposition 3'. — Quels que soient les nombres entier n, impair (pair) $\geqslant 3$, m $(1 \leqslant m < n)$ et les trois nombres a, b, c

[1] a, b, c, ... étant des nombres entiers, $D(a, b, c, \ldots)$ désigne leur plus grand commun diviseur.

de la suite 1, 2, ..., n, dont l'un au moins est $\leqslant m$ et l'un au moins est $> m$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\,2 \ldots m)\,(m+1 \ldots n)$, $T = (a\,b\,c)$ constituent une base du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$), c'est que $D(m, n-m, d) = 1$, d désignant la valeur absolue de la différence des deux nombres du système a, b, c qui appartiennent au même cycle de S.

Proposition 4. — Quels que soient le nombre entier $n \geqslant 7$ et les quatre nombres a, b, c, d de la suite 1, 2, ..., n, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\,2 \ldots n)$, $T = (a\,b\,c\,d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que $D(\overline{ab}, \overline{ac}, \overline{ad}, n) = 1$ et que l'on n'ait pas simultanément $\overline{ab} = \overline{cd}$, $\overline{bc} = \overline{da}$.

Proposition 5. — Quels que soient le nombre pair (impair) $n \geqslant 9$ et les cinq nombres a, b, c, d, e de la suite 1, 2, ..., n, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\,2 \ldots n)$, $T = (a\,b\,c\,d\,e)$ constituent une base du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$), c'est que $D(\overline{ab}, \overline{ac}, \overline{ad}, \overline{ae}, n) = 1$.

Nous avons également démontré que quel que soit le nombre entier $n \geqslant 5$ ainsi que les cinq nombres a, b, c, d, e de la suite 1, 2, ..., n, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\,2 \ldots n)$, $T = (a\,b)\,(c\,d\,e)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que $D(\overline{ab}, \overline{cd}, \overline{ce}, n) = 1$.

En nous appuyant sur les résultats précités, nous établirons plusieurs nouveaux critères permettant de discerner les bases du groupe symétrique et du groupe alterné.

Proposition I. — Quels que soient le nombre entier $n \geqslant 9$ ainsi que les sept nombres a, b, c, d, e, f, g de la suite 1, 2, ..., n, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\,2 \ldots n)$, $T = (a\,b)\,(c\,d\,e\,f\,g)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que

$$D(\overline{ab}, \overline{cd}, \overline{ce}, \overline{cf}, \overline{cg}, n) = 1\ . \qquad (1)$$

Démonstration: La condition est nécessaire, car, si elle n'est pas vérifiée, les deux substitutions S, T sont imprimitives.

La condition est suffisante. En effet, supposons que (1) a lieu. On a

$$T^5 = (a\,b)\ , \qquad T^6 = (c\,d\,e\,f\,g)\ .$$

Si $D(\overline{ab},\ n) = k_1 = 1$, les deux substitutions $(a\ b)$ et S engendrent le groupe $\mathfrak{S}_n$, d'après la proposition 2. Donc, S, T est bien une base de $\mathfrak{S}_n$. De même, si $D(\overline{cd}, \overline{ce}, \overline{cf}, \overline{cg}, n) = k_2 = 1$, les deux substitutions S et $(c\,d\,e\,f\,g)$ engendrent le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, d'après la proposition 5. Donc, comme T est de classe impaire, S, T est bien une base de $\mathfrak{S}_n$.

Soit $k_1 > 1$, $k_2 > 1$. On a

$$S^{c-a}\,(a\,b)\,S^{-c+a} = (c\,b_1)\ , \qquad 1 \leqslant b_1 \leqslant n\ , \qquad \overline{cb_1} = \overline{ab}\ .$$

D'après les propositions 1 et 2, les deux substitutions $(c\ b_1)$ et $(c\,d\,e\,f\,g)$ engendrent toujours le groupe symétrique des substitutions des éléments qu'elles permutent. Ce groupe comprend les transpositions $(c\ b_1)$, $(c\ d)$, $(c\ e)$, $(c\ f)$, $(c\ g)$ et, d'après (1) et le lemme 1, en composant S avec ces diverses transpositions, on obtient le groupe $\mathfrak{S}_n$. Il s'ensuit que S, T est bien une base de $\mathfrak{S}_n$, c.q.f.d.

Proposition II. — Quels que soient le nombre entier $n \geqslant 7$ ainsi que les sept nombres a, b, c, d, e, f, g de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b\ c)\ (d\ e\ f\ g)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que

$$D(\overline{ab},\ \overline{ac},\ \overline{de},\ \overline{df},\ \overline{dg},\ n) = 1\ . \qquad (1)$$

Démonstration: La condition est nécessaire, car, si elle n'est pas vérifiée, les substitutions S, T sont imprimitives.

La condition est suffisante. En effet, supposons que (1) a lieu. On a

$$T^4 = (a\,b\,c)\ , \qquad T^9 = (d\,e\,f\,g)\ .$$

Si l'une au moins de ces deux substitutions engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, la proposition est démontrée. Supposons que tel n'est pas le cas. On a

$$S^{d-a}\,T\,S^{-d+a} = (d\,b_1\,c_1)\ , \quad 1 \leqslant b_1 \leqslant n\ , \quad 1 \leqslant c_1 \leqslant n\ , \quad \overline{db_1} = \overline{ab}\ , \quad \overline{dc_1} = \overline{ac}\ .$$

D'après les propositions 1, 3 et 3', les substitutions $(d\ b_1\ c_1)$ et $(d\ e\ f\ g)$ engendrent toujours le groupe symétrique des substitutions des éléments qu'elles permutent. Ce groupe comprend les transpositions $(d\ b_1)$, $(d\ c_1)$, $(d\ e)$, $(d\ f)$, $(d\ g)$ et, d'après (1) et le lemme 1, en composant S avec ces diverses transpositions, on obtient le groupe $\mathfrak{S}_n$. Donc S, T est bien une base de $\mathfrak{S}_n$, c.q.f.d.

Proposition III. — Quels que soient le nombre pair (impair) $n \geqslant 9$ ainsi que les huit nombres a, b, c, d, e, f, g, h de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b\ c)\ (d\ e\ f\ g\ h)$ constituent une base du groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$, c'est que

$$D\,(\overline{ab},\ \overline{ac},\ \overline{de},\ \overline{df},\ \overline{dg},\ \overline{dh},\ n) = 1. \qquad (1)$$

Démonstration: La condition est nécessaire, car, si elle n'est pas vérifiée, les deux substitutions S, T sont imprimitives.

La condition est suffisante. En effet, supposons que (1) a lieu. On a

$$T^{10} = (a\ b\ c)\ , \qquad T^{6} = (d\ e\ f\ g\ h)\ .$$

Si l'une au moins de ces deux substitutions engendre avec S le groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$, la proposition est démontrée. Supposons que tel n'est pas le cas. On a

$$S^{d-a}(a\ b\ c)\,S^{-d+a} = (d\ b_1\ c_1)\ ,\ 1 \leqslant b_1 \leqslant n\ ,\ 1 \leqslant c_1 \leqslant n\ ,\ \overline{db_1} = \overline{ab}\ ,\ \overline{dc_1} = \overline{ac}\ .$$

D'après les propositions 1, 3 et 3', les deux substitutions $(d\ b_1\ c_1)$ et $(d\ e\ f\ g\ h)$ engendrent toujours le groupe alterné des substitutions des éléments qu'elles permutent. Ce groupe contient les substitutions $(d\ b_1\ c_1)$, $(d\ b_1\ e)$, $(d\ b_1\ f)$, $(d\ b_1\ g)$ et, d'après (1) et le lemme 2, en composant S avec ces diverses substitutions, on obtient le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. Donc S, T est bien une base de $\mathfrak{S}_n(\mathfrak{A}_n)$, c.q.f.d.

Proposition IV. — Quels que soient le nombre entier $n \geqslant 10$ ainsi que les dix nombres $a, b, c, d, e, f, g, h, i, j$ de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les

deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b)\ (c\ d\ e)\ (f\ g\ h\ i\ j)$ engendrent le groupe $\mathfrak{S}_n$, c'est que

$$D(\overline{ab},\ \overline{cd},\ \overline{ce},\ \overline{fg},\ \overline{fh},\ \overline{fi},\ \overline{fj},\ n) = 1\ . \qquad (1)$$

Démonstration: La condition est nécessaire. En effet, si elle n'est pas satisfaite, les substitutions S, T sont imprimitives.

La condition est suffisante. En effet, supposons que (1) a lieu. On a

$$T^{15} = (a\,b)\ ,\quad T^{10} = (c\,d\,e)\ ,\quad T^{6} = (f\,g\,h\,i\,j)\ .$$

Si l'une au moins de ces trois substitutions engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, la proposition est démontrée. Supposons que tel n'est pas le cas. On a

$$S^{f-a}(a\,b)\,S^{-f+a} = (f\,b_1)\ ,\quad S^{f-c}(c\,d\,e)\,S^{-f+c} = (f\,d_1\,e_1)\ ,$$
$$1 \leqslant b_1 \leqslant n\ ,\quad 1 \leqslant d_1 \leqslant n\ ,\quad 1 \leqslant e_1 \leqslant n\ ,$$
$$\overline{fb_1} = \overline{ab}\ ,\quad \overline{fd_1} = \overline{cd}\ ,\quad \overline{fe_1} = \overline{ce}\ .$$

D'après les propositions 1, 2, 3 et 3′, en composant les trois substitutions $(f\ b_1)$, $(f\ d_1\ e_1)$, $(f\ g\ h\ i\ j)$, on obtient toujours le groupe symétrique des substitutions des éléments qu'elles permutent. Ce groupe contient les transpositions $(f\ b_1)$, $(f\ d_1)$, $(f\ e_1)$, $(f\ g)$, $(f\ h)$, $(f\ i)$, $(f\ j)$ et, d'après (1) et le lemme 1, en composant S avec ces diverses transpositions, on obtient le groupe $\mathfrak{S}_n$. Donc S, T est bien une base de $\mathfrak{S}_n$, c.q.f.d.

Proposition V. — Quels que soient le nombre entier $n \geqslant 12$ ainsi que les douze nombres $a, b, c, d, e, f, g, h, i, j, k, l$ de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b\ c)\ (d\ e\ f\ g)\ (h\ i\ j\ k\ l)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que

$$D(\overline{ab},\ \overline{ac},\ \overline{de},\ \overline{df},\ \overline{dg},\ \overline{hi},\ \overline{hj},\ \overline{hk},\ \overline{hl},\ n) = 1\ . \qquad (1)$$

Démonstration: La condition est nécessaire, car, si elle n'est pas satisfaite, les substitutions S, T sont imprimitives.

La condition est suffisante. En effet, supposons que (1) a lieu. On a

$$T^{40} = (a\,b\,c)\ ,\quad T^{45} = (d\,e\,f\,g)\ ,\quad T^{36} = (h\,i\,j\,k\,l)\ .$$

Si l'une au moins de ces trois substitutions engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, la proposition est démontrée. Supposons que tel n'est pas le cas. On a

$$S^{h-a}(a\,b\,c)\,S^{-h+a} = (h\,b_1\,c_1)\ , \qquad S^{h-d}(d\,e\,f\,g)\,S^{-h+d} = (h\,e_1\,f_1\,g_1)\ ,$$

b_1, c_1, e_1, f_1, g_1 étant des nombres déterminés de la suite $1, 2, \ldots, n$, tels que

$$\overline{hb_1} = \overline{ab}\ , \quad \overline{hc_1} = \overline{ac}\ , \quad \overline{he_1} = \overline{de}\ , \quad \overline{hf_1} = \overline{df}\ , \quad \overline{hg_1} = \overline{dg}\ .$$

On voit sans peine que les trois substitutions $(h\ b_1\ c_1)$, $(h\ e_1\ f_1\ g_1)$, $(h\ i\ j\ k\ l)$ engendrent toujours le groupe symétrique des substitutions des éléments qu'elles permutent, groupe qui contient les transpositions $(h\ b_1)$, $(h\ c_1)$, $(h\ e_1)$, $(h\ f_1)$, $(h\ g_1)$, $(h\ i)$, $(h\ j)$, $(h\ k)$, $(h\ l)$ et, d'après (1) et le lemme 1, en composant S avec ces diverses transpositions, on obtient le groupe $\mathfrak{S}_n$. Donc S, T est une base de $\mathfrak{S}_n$, c.q.f.d.

Par la même méthode, on démontre sans peine les deux propositions plus générales suivantes que nous nous bornons à énoncer ici:

Proposition VI. — Quels que soient le nombre entier positif $n \geqslant 5$, les deux nombres a, b de la suite $1, 2, \ldots, n$, ainsi que les $r \geqslant 1$ nombres impairs > 1: $m_1, m_2, \ldots, m_r$, premiers deux à deux et avec $\overline{ab}$ $(m_1 + m_2 + \ldots + m_r + 2 = m \leqslant n)$, et quels que soient les $m - 2$ nombres $a_{i1}, a_{i2}, \ldots, a_{im_i}$ $(\neq a, b)$ de la suite $1, 2, \ldots, n$ $(i = 1, 2, \ldots, r)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b)\,(a_{11}\,a_{12}\ \ldots\ a_{1m_1})\ \ldots\ (a_{r1}\,a_{r2}\ \ldots\ a_{rm_r})$ constituent une base du groupe $\mathfrak{S}_n$, c'est que

$$D(\overline{ab},\ \overline{a_{11}\,a_{12}},\ \ldots,\ \overline{a_{11}\,a_{1m_1}},\ \ldots,\ \overline{a_{r1}\,a_{r2}},\ \ldots,\ \overline{a_{r1}\,a_{rm_r}},\ n) = 1\ .$$

Proposition VII. — Quels que soient le nombre entier $n \geqslant 5$, les trois nombres a, b, c de la suite $1, 2, \ldots, n$, les $r \geqslant 1$ nombres > 1: $m_1, m_2, \ldots, m_r, \not\equiv 0 \pmod 3$, premiers deux à deux et avec le nombre $D(\overline{ab}, \overline{ac})$, $(m_1 + m_2 + \ldots + m_r + 3 = m \leqslant n)$, ainsi que les $m - 3$ nombres $a_{i1}, a_{i2}, \ldots, a_{im_i}$ $(\neq a, b, c)$ de la

suite 1, 2, ..., n, ($i = 1, 2, \ldots, r$), la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a\ b\ c)\ (a_{11}\ a_{12}\ \ldots\ a_{1m_1})\ \ldots\ (a_{r1}\ a_{r2}\ \ldots\ a_{rm_r})$ constituent une base du groupe $\mathfrak{S}_n$ ou du groupe $\mathfrak{A}_n$, c'est que

$$D(\overline{ab},\ \overline{ac},\ \overline{a_{11}a_{12}},\ \ldots,\ \overline{a_{11}a_{1m_1}},\ \ldots,\ \overline{a_{r1}a_{r2}},\ \ldots,\ \overline{a_{r1}a_{rm_r}},\ n) = 1\ .$$

Voici encore quelques propositions et remarques concernant les bases du groupe symétrique et du groupe alterné.

Proposition VIII. — Quel que soit le nombre entier $n > 3$, deux substitutions S, T du second ordre et de degré n ne sauraient constituer une base du groupe $\mathfrak{S}_n$ ni du groupe $\mathfrak{A}_n$.

Démonstration: Soient S et T deux substitutions du second ordre et de degré n, dont les éléments forment un ensemble E. Si elles ne sont pas connexes, elles ne sauraient engendrer ni le groupe $\mathfrak{S}_n$ ni le groupe $\mathfrak{A}_n$. *Supposons qu'elles sont connexes.* Le nombre total de cycles de premier ordre faisant partie de ces deux substitutions ne saurait alors être > 2.

Si aucune des substitutions S, T ne contient de cycles du premier ordre, n est un nombre pair et l'on voit sans peine, par l'induction, qu'il existe une suite $a_1, a_2, \ldots, a_n$ formée de tous les éléments de E, telle que

$$S = (a_1\,a_2)\,(a_3\,a_4)\ \ldots\ (a_{n-1}\,a_n)\ , \qquad T = (a_2\,a_3)\,(a_4\,a_5)\ \ldots\ (a_n\,a_1)\ .$$

Soit

$$E_1 = \{a_1,\ a_3,\ \ldots,\ a_{n-1}\}\ , \qquad E_2 = \{a_2,\ a_4,\ \ldots,\ a_n\}\ .$$

Chacune des substitutions S, T transforme les ensembles E_1, E_2 l'un dans l'autre. Les substitutions S, T sont donc imprimitives et ne sauraient, de ce fait, constituer une base ni de $\mathfrak{S}_n$ ni de $\mathfrak{A}_n$.

Supposons maintenant que n est pair $\geqslant 4$ et que l'une des substitutions S, T, par exemple S, contient deux cycles du premier ordre. La substitution T ne contient alors aucun cycle du premier ordre et l'on voit sans peine qu'il existe une suite $a_1, a_2, \ldots, a_n$ formée de tous les éléments de E, telle que

$$S = (a_1)\,(a_2\,a_3)\,(a_4\,a_5)\ \ldots\ (a_{n-2}\,a_{n-1})\,(a_n)\ , \qquad T = (a_1\,a_2)\,(a_3\,a_4)\ \ldots\ (a_{n-1}\,a_n)\ .$$

Posons

$$E_1 = \{a_1, a_n\}, \quad E_2 = \{a_2, a_{n-1}\}, \quad E_3 = \{a_3, a_{n-2}\}, \ \ldots,$$

$$E_{\frac{n}{2}} = \{a_{\frac{n}{2}}, \ a_{\frac{n}{2}+1}\}.$$

Il est clair que chacune des substitutions S, T transforme tout ensemble E_i en un ensemble $E_j\left(1 \leqslant i \leqslant \frac{n}{2}, \ 1 \leqslant j \leqslant \frac{n}{2}\right)$. Donc, dans ce cas aussi, les substitutions S, T sont imprimitives et ne sauraient, de ce fait, engendrer ni le groupe $\mathfrak{S}_n$ ni le groupe $\mathfrak{A}_n$.

Supposons, enfin, que n est impair $\geqslant 5$. Alors, S et T étant connexes, chacune de ces substitutions doit contenir un cycle du premier ordre et un seul, et il existe une suite $a_1, a_2, \ldots, a_n$, formée de tous les éléments de E, telle que

$$S = (a_1)(a_2\,a_3)(a_4\,a_5) \ldots (a_{n-1}\,a_n), \quad T = (a_1\,a_2)(a_3\,a_4) \ldots (a_{n-2}\,a_{n-1})(a_n).$$

Ces deux substitutions engendrent un groupe d'ordre $2n$, composé des substitutions S, ST, STS, $(ST)^2$, ..., $(ST)^n = 1$. Et comme $2n < \frac{n!}{2}$, quel que soit le nombre impair $n > 3$, S et T ne sauraient constituer une base ni de $\mathfrak{S}_n$ ni de $\mathfrak{A}_n$.

La proposition est ainsi établie.

Proposition IX. — Quel que soit le nombre pair (impair) $n>3$, il existe pour toute substitution circulaire S du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$ au moins une substitution circulaire T qui forme avec S une base du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$.

Démonstration: Il suffit évidemmcnt d'établir la proposition pour une substitution circulaire S quelconque, par exemple pour $S = (1\ 2\ \ldots\ n)$.

Supposons d'abord que n est pair. Posons

$$T = (2\ 4\ 6\ \ldots\ n\ 3\ 5\ 7\ \ldots\ n-1\ 1).$$

Je dis que les deux substitutions S et T constituent une base de $\mathfrak{S}_n$. En effet, on a

$$S^{-1}\,T\,S^{-1} = (1\ 2)$$

et, d'après la proposition 1, les deux substitutions S et (1 2) engendrent le groupe $\mathfrak{S}_n$. Notre proposition est donc établie pour n pair.

Soit à présent n un nombre impair: $n = 2k + 1$, $(k \geqslant 2)$. Posons

$$T = (1\ k+2\ 3\ k+4\ 4\ k+5\ \ldots\ k\ 2k+1\ k+1\ 2\ k+3)\ .$$

En particulier, si $k = 2$, $T = (14325)$.

On vérifie sans peine que $T S^k = (1\ 2\ 3)$ et, d'après la proposition 1, les deux substitutions S et (1 2 3) engendrent le groupe $\mathfrak{A}_n$, ce qui démontre notre proposition pour n impair.

Remarque: Quel que soit le nombre pair (impair) $n > 2$, il existe pour toute substitution circulaire du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) au moins une substitution circulaire T qui ne forme pas avec S une base du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$). Telle est, par exemple, la substitution $T = S^{-1}$.

Remarque: Si $3 \leqslant n \leqslant 6$, deux substitutions d'ordre $\leqslant \frac{n}{2}$ faisant partie du groupe $\mathfrak{S}_n$ ne sauraient constituer une base de $\mathfrak{S}_n$. Cette propriété ne subsiste pas dans le cas général. Ainsi, les deux substitutions $S = (1\ 2\ 3)\ (4\ 5\ 6)$, $T = (3\ 6\ 7\ 8)$ engendrent le groupe $\mathfrak{S}_8$ et les deux substitutions $S = (1\ 2\ 3\ 4)\ (5\ 6\ 7\ 8)$, $T = (4\ 8\ 9\ 10)$ engendrent le groupe $\mathfrak{S}_{10}$.

Proposition X. — Quel que soit le nombre pair $n \geqslant 4$, une condition nécessaire pour que deux substitutions circulaires $S = (1\ 2\ \ldots\ n)$, $T = (a_1\ a_2\ \ldots\ a_n)$ du groupe $\mathfrak{S}_n$ puissent constituer une base de ce groupe, c'est que les deux substitutions S et $R = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$ en constituent une.

Démonstration: En effet, on a $T = R\,S\,R^{-1}$. La substitution T fait donc partie du groupe engendré par S et R, d'où résulte immédiatement notre proposition.

Problème 1: La condition énoncée dans la proposition X est-elle aussi suffisante ?

Problème 2: La proposition suivante a-t-elle lieu? Quel que soit le nombre entier $m > 1$, il existe un nombre entier N suffi-

samment grand (dépendant de m et non inférieur à m), tel que quel que soit le nombre entier $n \geqslant N$ ainsi que les m nombres $a_1, a_2, \ldots, a_m$ de la suite 1, 2, ..., n, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (a_1\ a_1\ \ldots\ a_m)$ constituent une base du groupe $\mathfrak{S}_n$ ou du groupe $\mathfrak{A}_n$, c'est qu'elles soient primitives.

Remarque: Soit n un nombre entier quelconque $\geqslant 3$, soit S une substitution non identique quelconque du groupe $\mathfrak{S}_n$ et soient $G_1, G_2, \ldots, G_r$ tous les sous-groupes propres de $\mathfrak{S}_n$ qui contiennent S. Envisageons l'ensemble des substitutions $M = \mathfrak{S}_n - (G_1 + G_2 + \ldots + G_r)$. Si M est vide, il n'existe aucune base du groupe $\mathfrak{S}_n$ qui contienne la substitution S. Ainsi, pour $n = 4$, si S est l'une des trois substitutions (1 2) (3 4), (1 3) (2 4), (1 4) (2 3), l'ensemble correspondant M est vide. Ce sont les seules substitutions du groupe $\mathfrak{S}_4$ jouissant de cette propriété. Comme nous l'avons démontré ailleurs, si $n > 4$, il n'existe aucune substitution non identique S du groupe $\mathfrak{S}_n$, pour laquelle l'ensemble M soit vide.

Par contre, si l'ensemble M n'est pas vide, quelle que soit la substitution T de M, elle constitue évidemment avec S une base de $\mathfrak{S}_n$. Ainsi la connaissance de tous les sous-groupes du groupe symétrique permet de concevoir sans peine toutes les bases de ce groupe. Pratiquement, cette méthode de rechercher les bases du groupe symétrique n'est applicable que pour de très petites valeurs de n.