Sur les bases du groupe symétrique et du groupe alternant.

Autor(en): **Piccard, Sophie**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **11 (1938-1939)**

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-11874

Sur les bases du groupe symétrique et du groupe alternant

Par SOPHIE PICCARD, Neuchâtel

1° Quel que soit le nombre entier $n \geqslant 3$ ($n > 3$), le groupe symétrique $\mathfrak{S}_n$ d'ordre $n!$ (le groupe alternant $\mathfrak{A}_n$ d'ordre $\frac{n!}{2}$) ne saurait être engendré par une seule de ses substitutions. Par contre, il existe des couples S, T de substitutions de $\mathfrak{S}_n(\mathfrak{A}_n)$, tels que toute substitution de $\mathfrak{S}_n(\mathfrak{A}_n)$ peut être obtenue en composant S et T. Nous appelons *base* du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$ tout couple de substitutions de $\mathfrak{S}_n(\mathfrak{A}_n)$ jouissant de cette propriété. Quel que soit le nombre entier $n \geqslant 3$ ($n > 3$), le nombre total $N(N')$ de bases du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$ est un invariant de ce groupe. Nous avons démontré ailleurs[1]) que le nombre $N(N')$ est un multiple de $\frac{n!}{2}\left(\frac{n!}{4}\right)$. Le but de la présente note est d'établir quelques critères généraux permettant de juger si deux substitutions données appartenant au groupe $\mathfrak{S}_n(\mathfrak{A}_n)$ constituent ou non une base de ce groupe.

Nous désignons, en général, par les nombres 1, 2, ..., n les éléments d'une substitution de degré n.

Une condition nécessaire et suffisante pour que deux substitutions S et T de $\mathfrak{S}_n(\mathfrak{A}_n)$ constituent une base de ce groupe est qu'elles n'appartiennent toutes deux à aucun vrai sous-groupe de $\mathfrak{S}_n(\mathfrak{A}_n)$.

Si deux substitutions S et T constituent une base de $\mathfrak{S}_n(\mathfrak{A}_n)$, quelle que soit la substitution R de $\mathfrak{S}_n(\mathfrak{A}_n)$, les deux substitutions transformées de S et de T par la substitution R constituent évidemment aussi une base de $\mathfrak{S}_n(\mathfrak{A}_n)$.

Nous disons que deux substitutions S et T de degré n sont connexes s'il n'existe aucun sous-ensemble propre E' de l'ensemble $E = \{1, 2, \ldots n\}$, tel que les éléments de E' constituent un système fini de cycles aussi bien dans S que dans T. On établit sans peine qu'une condition nécessaire, mais pas suffisante, pour que deux substitutions S et T constituent une base de $\mathfrak{S}_n(\mathfrak{A}_n)$ est que ces deux substitutions soient connexes.

On voit aussi aisément que quelles que soient deux substitutions semblables S et S' du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$, le nombre de bases de $\mathfrak{S}_n(\mathfrak{A}_n)$ comprenant la substitution S est le même que le nombre de bases comprenant la substitution S'. Soit S, T une base quelconque du groupe $\mathfrak{S}_n(\mathfrak{A}_n)$

[1]) Časopis pro pestováni Matematiky a Fysiky, Praha, 1938.

comprenant la substitution S. Les deux substitutions S et S' étant semblables, nous pouvons toujours les écrire sous la forme

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

On a $S' = USU^{-1}$.[2])

Posons $T' = UTU^{-1}$.

Les deux substitutions S', T' constituent également une base de $\mathfrak{S}_n(\mathfrak{A}_n)$. Pour trouver toutes les bases de $\mathfrak{S}_n(\mathfrak{A}_n)$, il suffit donc de connaître les bases de $\mathfrak{S}_n(\mathfrak{A}_n)$ qui comprennent une substitution fixe quelconque de chaque classe de substitutions semblables appartenant au groupe envisagé.

2° *Proposition 1.* Quel que soit le nombre entier $n \geqslant 3$, les deux substitutions $S = (1\ 2\ \dots\ n)$, $T = (1\ 2)$ constituent une base du groupe $\mathfrak{S}_n$.

Démonstration. On a, pour toute valeur de l'entier k,

$S^k T\ S^{-k} = (1+k\ 2+k)$, les nombres $>n$ devant être réduits mod. n. Donc les transpositions

$$(1\ 2),\ (2\ 3),\ \dots,\ (n-1\ n) \qquad (*)$$

font toutes partie du groupe engendré par S et T.

Je dis que ces transpositions (*) engendrent le groupe $\mathfrak{S}_n$, quel que soit $n \geqslant 2$.

En effet, cette propriété est évidemment vraie pour $n = 2$. Soit à présent n un nombre entier quelconque > 2 et supposons que notre propriété est juste pour $n - 1$. Montrons qu'elle est encore vraie pour n.

D'après notre hypothèse, les transpositions

$$(1\ 2),\ (2\ 3),\ \dots,\ (n-2\ n-1)$$

engendrent le groupe $\mathfrak{S}_{n-1}$. Comme les transpositions $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n-1)$ font partie de ce groupe et comme $(1\ n-1)\ (n-1\ n)\ (1\ n-1) = (1\ n)$, nous voyons que les $n-1$ transpositions

$$(1\ k),\ (k = 2, 3, \dots, n)\ , \qquad (**)$$

peuvent être obtenues en composant les transpositions (*). Or, on sait que les $n-1$ transpositions (**) engendrent le groupe $\mathfrak{S}_n$. Il en est donc de même des transpositions (*). Il en résulte que S et T constituent bien une base de $\mathfrak{S}_n$, c.q.f.d.

---

[2]) Les substitutions successives de la composition doivent être effectuées de droite à gauche.

Corollaire[3]). Quels que soient les nombres entiers $n \geqslant 3$ et $m \geqslant 1$ et $\leqslant n$, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (m\ m+1)$, où $m+1$ doit être remplacé par 1 si $m = n$, constituent une base du groupe $\mathfrak{S}_n$.

Proposition 2. Quel que soit le nombre entier $n \geqslant 3$, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (1\ 2\ 3)$ engendrent le groupe $\mathfrak{A}_n$, si n est impair, ou le groupe $\mathfrak{S}_n$, si n est pair.

Démonstration. Il suffit de montrer que, quel que soit le nombre entier $n \geqslant 3$, le groupe $\mathfrak{A}_n$ est compris dans le groupe engendré par les deux substitutions S et T. Remarquons, à cet effet, que quel que soit le nombre entier k, on a $S^k T\ S^{-k} = (1+k\ \ 2+k\ \ 3+k)$, les nombres $> n$ devant être réduits mod. n. Donc les substitutions

$$(1\ 2\ 3),\ (2\ 3\ 4),\ \ldots,\ (n-2\ \ n-1\ \ n) \qquad (*)$$

font toutes partie du groupe engendré par S et T. Je dis que ces $n-2$ substitutions engendrent le groupe $\mathfrak{A}_n$. Cette propriété a évidemment lieu pour $n = 3$. Soit à présent n un nombre entier quelconque > 3 et supposons que notre propriété a lieu pour $n-1$. Montrons qu'elle a aussi lieu pour n. En vertu de notre hypothèse, les substitutions $(1\ 2\ 3)$, $(2\ 3\ 4)$, $\ldots$, $(n-3\ \ n-2\ \ n-1)$ engendrent le groupe $\mathfrak{A}_{n-1}$. Ce groupe contient les substitutions $(1\ 2\ 3)$, $(1\ 2\ 4)$, $\ldots$, $(1\ 2\ n-1)$ ainsi que la substitution $R = (2\ n-1)\ (1\ n-2)$.

Or, on a $\qquad R\ (n-2\ \ n-1\ \ n)\ R^{-1} = (1\ 2\ n).$

Ainsi les $n-2$ substitutions

$$(1\ 2\ 3),\ (1\ 2\ 4),\ \ldots,\ (1\ 2\ n) \qquad (**)$$

s'obtiennent en composant les substitutions (*). Or, les substitutions (**) engendrent, comme on sait, le groupe $\mathfrak{A}_n$. Il s'ensuit que $\mathfrak{A}_n$ fait bien partie du groupe engendré par S et T, ce qui démontre la proposition énoncée.

Corollaire. Quels que soient les nombres entiers $n > 3$ et $m \geqslant 1$ et $\leqslant n$, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (m\ m+1\ \ m+2)$, où les nombres $> n$ doivent être réduits mod. n, constituent une base du groupe $\mathfrak{S}_n$, si n est pair, ou du groupe $\mathfrak{A}_n$, si n est impair.

Proposition 3. Quels que soient les nombres entiers $n > 2$ et $k > 1$ et $< n$, les deux substitutions $S = (1\ 2\ \ldots\ n)$ et $T = (1\ 2\ \ldots\ k)$ constituent une base du groupe $\mathfrak{S}_n$, si l'un au moins des nombres n, k, est pair, ou une base du groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs.

---

[3]) Nous nous bornons à énoncer les corollaires dont la démonstration ne présente aucune difficulté.

Démonstration. Dans le cas particulier où $k = 2$, notre proposition se réduit à la proposition 1. Elle se réduit à la proposition 2 pour $k = 3$ et nous l'avons déjà établie dans ces deux cas. Soit à présent k un nombre entier quelconque > 3 et $< n$. On a, quel que soit le nombre entier m: $S^m T\ S^{-m} = (1+\mathrm{m}\ 2+m \ldots k+m)$ (les nombres $> n$ devant être réduits mod. n). Je dis que les substitutions

$$(1\ 2 \ldots k), (2\ 3 \ldots k+1), \ldots, (1+n-k\ 2+n-k \ldots n) \qquad (*)$$

engendrent le groupe $\mathfrak{S}_n$, si k est pair, ou le groupe $\mathfrak{A}_n$, si k est impair.

En effet, supposons d'abord que $n = k+1$.

Posons $T_1 = (2\ 3 \ldots k+1)$.

On a $T_1 = T\ (1\ k\ k+1)$.

Donc $(1\ k\ k+1) = T^{-1}T_1$ et $T_1^2\,(1\ k\ k+1)\ T_1^{-2} = (1\ 2\ 3)$.

D'après la proposition 2, la substitution (1 2 3) forme avec T une base du groupe $\mathfrak{S}_k$, si le nombre k est pair, ou du groupe $\mathfrak{A}_k$, si k est impair. Le groupe engendré par les substitutions (1 2 3) et T contient donc les substitutions (1 2 3), (1 2 4), ..., (1 2 k). Or, (1 2 k) (1 k $k+1$) (1 k 2) = (2 1 $k+1$), $(2\ 1\ k+1)^2 = (1\ 2\ k+1)$ et l'on sait que les substitutions (1 2 3), (1 2 4), ..., (1 2 $k+1$) engendrent le groupe $\mathfrak{A}_{k+1}$. Il en résulte que les deux substitutions T et T_1 engendrent bien le groupe $\mathfrak{S}_{k+1}$, si k est pair, ou le groupe $\mathfrak{A}_{k+1}$, si k est impair.

Soit à présent n un nombre entier quelconque $> k+1$ et supposons que nous avons déjà établi la proposition pour $n-1$. Démontrons la pour n. D'après notre hypothèse, les substitutions

$$(1\ 2 \ldots k), (2\ 3 \ldots k+1), \ldots, (n-k\ n-k+1 \ldots n-1) \qquad (**)$$

engendrent le groupe $\mathfrak{S}_{n-1}$, si k est pair, ou le groupe $\mathfrak{A}_{n-1}$, si k est impair. Le groupe engendré par les substitutions (**) contient donc en tout cas les substitutions (1 2 3), (1 2 4), ..., (1 2 $n-1$), ainsi que les deux substitutions

$R = (n-k+1\ \ n-2\ \ n-3 \ldots n-k+2)$ et $Q = (1\ n-k+1)\,(2\ n-1)$.

Posons $T_2 = (n-k+1\ \ n-k+2 \ldots n)$.

On a $T_2R = (n-k+1\ \ n-1\ \ n)$ et $Q\,T_2R\,Q^{-1} = (1\ 2\ n)$.

Les substitutions (1 2 3), (1 2 4), ..., (1 2 n) font donc toutes partie du groupe engendré par les substitutions (*) et par suite ces substitutions engendrent bien le groupe $\mathfrak{S}_n$, si k est pair, ou le groupe $\mathfrak{A}_n$, si k est impair. Il en résulte immédiatement que si l'un au moins des nombres n, k est pair, les deux substitutions S et T forment une base du groupe $\mathfrak{S}_n$ et si ces deux nombres n et k sont impairs, S, T est une base du groupe $\mathfrak{A}_n$, c.q.f.d.

Corollaire 1. Dans le cas particulier où $n = k+1$, les deux substitutions S et T définies dans l'énoncé de la proposition 3 forment nécessairement une base du groupe $\mathfrak{S}_n$, puisque l'un des nombres k, $k+1$ est pair.

Corollaire 2. Quels que soient les nombres entiers $n > 2$, $m \geqslant 0$ et $< n$ et $k > 1$ et $< n$, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (m+1\ m+2\ \ldots\ m+k)$ (où les nombres $> n$ doivent être réduits mod. n) constituent une base du groupe $\mathfrak{S}_n$, si l'un au moins des nombres n, k est pair, ou une base du groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs.

Corollaire 3 [4]). Quels que soient les nombres entiers $n \geqslant 3$ et $k > 1$ et $< n$, les deux substitutions $S = (1\ 2\ \ldots\ k)$, $T = (i\ k+1\ \ldots\ n)$ $(1 \leqslant i \leqslant k)$ constituent une base du groupe $\mathfrak{S}_n$, si l'un au moins des nombres n, k est pair, ou du groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs.

C'est une conséquence immédiate de la proposition 3 et des relations $T' = S^{k-i}\ T\ S^{-k+i} = (k\ k+1\ \ldots\ n)$ et $ST' = (1\ 2\ \ldots\ n)$.

Dans le cas particulier où $n = k+1$, la substitution T est de classe impaire et, par suite, les deux substitutions $S = (1\ 2\ \ldots\ n-1)$, $T = (i\ n)$ $(1 \leqslant i \leqslant n-1)$ constituent toujours une base du groupe $\mathfrak{S}_n$.

3° *Proposition 4.* La condition nécessaire et suffisante pour que deux substitutions de la forme $S = (1\ 2\ \ldots\ n)$, $T = (a\ b)$, où a, b sont deux nombres distincts de la suite 1, 2, ..., n, constituent une base du groupe $\mathfrak{S}_n$ est que le plus grand commun diviseur $D(|\ a-b\ |, n)$ des deux nombres $|\ a-b\ |$ et n soit égal à l'unité.

Démonstration. Nous pouvons toujours choisir les notations de façon à avoir $a < b$. On a alors $S^{-a+1}\ T\ S^{a-1} = (1\ b-a+1)$, où $b-a+1 \geqslant 2$. Posons $b-a = k$ $(k \geqslant 1$ et $< n)$. Les deux couples de substitutions $(1\ 2\ \ldots\ n)$, $(a\ b)$ et $(1\ 2\ \ldots\ n)$, $(1\ 1+k)$ engendrent des groupes simplement isomorphes. Pour établir notre proposition, il suffit donc de prouver que la condition nécessaire et suffisante pour que deux substitutions de la forme $S = (1\ 2\ \ldots\ n)$, $T = (1\ 1+k)$ constituent une base du groupe $\mathfrak{S}_n$ est que le plus grand commun diviseur des deux nombres n et k soit égal à l'unité.

La condition est nécessaire. En effet, supposons qu'elle n'est pas vérifiée et soit $D(k, n) = m > 1$. Soit $n = n'\,m$.

Posons $E = \{1, 2, \ldots, n\}$; $E_i = \{i, i+m, i+2m, \ldots, i+(n'-1)m\}$, $(i = 1, 2, \ldots m)$.

Il est clair que $E = \sum_{i=1}^{m} E_i$ et que les ensembles E_i sont disjoints deux

[4]) Ce corollaire a déjà été établi, par une autre voie, par *M. Hoyer.* Voir Math. Annalen 46 (1895), p. 541, lemme 1.

à deux. Or, il résulte immédiatement de nos hypothèses sur les substitutions S et T que chacune de ces substitutions transforme tout ensemble E_i en un ensemble E_j ($1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant m$). Donc le groupe engendré par les substitutions S et T n'est pas primitif et comme le groupe $\mathfrak{S}_n$ (aussi bien que le groupe $\mathfrak{A}_n$) est primitif, les deux substitutions S et T ne sauraient constituer une base de ce groupe. La condition énoncée est donc bien nécessaire.

La condition est suffisante. En effet, soient

$$S = (1\ 2\ \ldots\ n),\quad T = (1\ 1+k)$$

deux substitutions, telles que $1 \leqslant k < n$ et que $D(k, n) = 1$. La suite des nombres $1, 1+k, 1+2k, \ldots, 1+(n-1)k$, réduits mod. n, contient alors tous les nombres de la suite $1, 2, \ldots, n$. Il existe donc un entier $m \geqslant 1$ et $\leqslant n-1$, tel que $1+m\,k \equiv 2 \pmod{n}$.

Or, on a $(T\,S^k)^{m-1}\,T\,(S^{-k}\,T)^{m-1} = (1\ 2)$.

En vertu de la proposition 1, les deux substitutions S et $(1\ 2)$ constituent une base du groupe $\mathfrak{S}_n$. Il en est donc de même des substitutions S, T, c.q.f.d.

Corollaire 1. Quelle que soit la permutation $a_1, a_2, \ldots, a_n$ des nombres $1, 2, \ldots, n$ et quels que soient les deux nombres entiers distincts i, j ($j > i$) compris au sens large entre 1 et n, la condition nécessaire et suffisante pour que les deux substitutions $P = (a_1\,a_2\,\ldots\,a_n)$, $Q = (a_i\,a_j)$ constituent une base du groupe $\mathfrak{S}_n$ est que $D(j-i, n) = 1$.

Corollaire 2. Quels que soient le nombre *premier* $n > 1$, la permutation $a_1, a_2, \ldots, a_n$ des nombres $1, 2, \ldots, n$ et les deux nombres entiers distincts a, b compris au sens large entre 1 et n, les deux substitutions $S = (a_1\,a_2\,\ldots\,a_n)$, $T = (a\,b)$ constituent une base du groupe $\mathfrak{S}_n$.

Corollaire 3. Quels que soient le nombre entier $n > 2$, la permutation $a_1, a_2, \ldots, a_n$ des nombres $1, 2, \ldots, n$ et les trois nombres entiers i, j, k vérifiant les relations $1 \leqslant k < n$, $1 \leqslant i \leqslant k$, $k+1 \leqslant j \leqslant n$, la condition nécessaire et suffisante pour que les deux substitutions

$$S = (a_1\,a_2\,\ldots\,a_k)\ (a_{k+1}\,a_{k+2}\,\ldots\,a_n),\quad T = (a_i a_j)$$

constituent une base du groupe $\mathfrak{S}_n$ est que $D(k, n-k) = 1$.

Cela résulte sans peine du corollaire 1 et du fait que la substitution ST est circulaire et égale à $(a_1 a_2 \ldots a_i\,a_{j+1} \ldots a_n a_{k+1}\,a_{k+2} \ldots a_j a_{i+1} \ldots a_k)$.

Dans le cas particulier où n est un nombre premier, deux substitutions connexes de la forme $S = (a_1\,a_2\,\ldots\,a_k)\,(a_{k+1}\,a_{k+2}\,\ldots\,a_n)$, $T = (a_i a_j)$ constituent toujours une base de $\mathfrak{S}_n$.

La proposition 4 et ses corollaires 1—3 permettent de trouver toutes les bases S, T du groupe $\mathfrak{S}_n (n > 1)$, dont l'une des substitutions T est une transposition.

Corollaire 4. Quels que soient les nombres entiers $n > 2$ et $k \geqslant 1$ et $< n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (1\ 2\ \ldots\ k)\ (k+1\ \ldots\ n)$ constituent une base du groupe $\mathfrak{S}_n$ est que $D(k, n-k) = 1$.

C'est une conséquence de la proposition 4 et de la relation $T^{m-1}S = (kn)$, m désignant le plus petit commun multiple des nombres k et $n-k$.

Proposition 5. Quel que soit le nombre entier n de la forme $n = rk$, où $r > 1$ et $k > 1$ sont deux nombres entiers, les deux substitutions $S = (1\ 2\ \ldots\ n)$

$$T = (1\ 2 \ldots k)\ (k+1\ k+2\ \ldots\ 2k)\ \ldots\ ((r-1)k+1\quad (r-1)k+2\ \ldots\ rk)$$

ne sauraient constituer une base du groupe $\mathfrak{S}_n (\mathfrak{A}_n)$.

Démonstration. On voit sans peine que le groupe engendré par les deux substitutions S et T ne saurait être primitif, puisque quel que soit $i = 1, 2, \ldots r$, chacune des substitutions S, T transforme tout ensemble $E_i = \{i, i+k, \ldots, i+(r-1)k\}$ en un ensemble de même nature, d'où résulte immédiatement notre proposition.

Proposition 6. Quels que soient les nombres entiers positifs $m_1, m_2, \ldots, m_r\ (r \geqslant 2)$, dont la somme $m_1 + m_2 + \ldots + m_r = n$, une condition nécessaire (mais pas suffisante) pour que les deux substitutions $S = (1\ 2\ \ldots\ n)$

$$T = (1\ 2\ \ldots\ m_1)\ (m_1+1\ m_1+2 \ldots m_1+m_2) \ldots (m_1+ \\ + m_2 + \ldots + m_{r-1} + 1\ \ldots\ m_1 + m_2 + \ldots + m_r)$$

constituent une base du groupe $\mathfrak{S}_n$ est que $D(m_1, m_2, \ldots, m_r) = 1$.

Démonstration. Supposons que la condition énoncée n'est pas vérifiée et soit $D(m_1, m_2, \ldots, m_r) = k > 1$. Le nombre k est alors aussi un diviseur *de* n. Soit $n = n'k$.

Posons $E_i = \{i, i+k, i+2k, \ldots, i+(n'-1)k\}$, $(i = 1, 2, \ldots, k)$.

On voit sans peine qu'aussi bien la substitution S que la substitution T transforment chaque ensemble $E_i (i < k)$ en E_{i+1} et l'ensemble E_k en E_1. Il s'ensuit que le groupe engendré par les substitutions S et T n'est pas primitif et, par conséquent, cela ne saurait être le groupe $\mathfrak{S}_n$ (ni le groupe $\mathfrak{A}_n$).

La condition énoncée est donc bien nécessaire. Mais elle n'est pas suffisante, comme le montre l'exemple suivant. Soit $S = (1\ 2\ 3\ 4\ 5\ 6)$, $T =$

(1 2) (3 4). On vérifie aisément que ces deux substitutions ne constituent ni une base du groupe $\mathfrak{S}_6$ ni une base du groupe $\mathfrak{A}_6$, mais qu'elles engendrent un sous-groupe d'ordre 120 de $\mathfrak{S}_6$.

Remarque. On déduit encore sans peine de la proposition 4 les trois corollaires suivants:

1° Soit $S = (1\ 2\ \ldots\ n)$ et soit T une substitution quelconque $\neq 1$ du groupe $\mathfrak{S}_n$. Soit $C = (a_1\, a_2\, \ldots\, a_r)$ un cycle quelconque d'ordre > 1 de la substitution T et soit a_i un élément quelconque de ce cycle $(1 \leqslant i \leqslant r)$. Formons la suite des nombres

$$|a_1 - a_i|, |a_2 - a_i|, \ldots, |a_{i-1} - a_i|, |a_{i+1} - a_i|, \ldots, |a_r - a_i|. \quad (*)$$

Procédons ainsi pour tous les cycles d'ordre > 1 de T et soit

$$b_1, b_2, \ldots, b_e \quad (**)$$

une suite formée de tous les nombres qui appartiennent aux différentes suites (*).

Une condition nécessaire pour que les deux substitutions S et T puissent constituer une base de $\mathfrak{S}_n$(ou de $\mathfrak{A}_n$) est que

$$D(b_1, b_2, \ldots, b_e, n) = 1.$$

2° Soit $S = (1\ 2\ \ldots\ n)$, $T = |\, i\, a_i\, |$, $(i = 1, 2, \ldots, n;\ 1 \leqslant a_i \leqslant n)$. Une condition nécessaire pour que ces deux substitutions puissent constituer une base de $\mathfrak{S}_n$ (ou de $\mathfrak{A}_n$) est que $D(a_1 - 1, a_2 - 2, \ldots, a_n - n, n) = 1$.

3° Soient S et T deux substitutions quelconques du groupe $\mathfrak{S}_n$. Soit $C = (a_1\, a_2\, \ldots\, a_r)$ un cycle quelconque d'ordre > 1 faisant partie de S ou de T et soit a_i un élément quelconque de ce cycle $(1 \leqslant i \leqslant r)$. Envisageons la suite des nombres

$$|a_1 - a_i|, |a_2 - a_i|, \ldots, |a_{i-1} - a_i|, |a_{i+1} - a_i|, \ldots, |a_r - a_i|. \quad (*)$$

Procédons de la sorte pour tous les cycles d'ordre > 1 aussi bien de S que de T et soit

$$b_1, b_2, \ldots, b_e \quad (**)$$

une suite formée de tous les nombres qui appartiennent aux différentes suites (*).

Une condition nécessaire pour que les deux substitutions S, T puissent constituer une base du groupe $\mathfrak{S}_n$ (ou du groupe $\mathfrak{A}_n$) est que l'on ait $D(b_1, b_2, \ldots, b_e, n) = 1$.

(Reçu le 11 juillet 1938.)