Artikel: Quelques propositions concernant les bases du groupe symétrique et du groupe alternant.

Autor: Piccard, Sophie

DOI: https://doi.org/10.5169/seals-12797

Quelques propositions concernant les bases du groupe symétrique et du groupe alternant

Par Sophie Piccard, Neuchâtel

I°

Il existe, pour toute valeur de l'entier $n \geqslant 3$ ($n \geqslant 4$), des couples de substitutions S, T faisant partie du groupe symétrique $\mathfrak{S}_n$ d'ordre $n!$ (du groupe alternant $\mathfrak{A}_n$ d'ordre $n!/2$), tels que toute substitution R du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) peut être obtenue en composant les deux substitutions S et T. Nous appelons *base* du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) tout couple de substitutions S, T jouissant de cette propriété.

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

Comme nous l'avons démontré ailleurs, quel que soit le nombre entier $n \geqslant 3$ ($n \geqslant 4$), il existe pour toute substitution non identique S du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) au moins une substitution T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) qui forme avec S une base du groupe considéré, à l'exception des trois substitutions (1 2) (3 4), (1 3) (2 4), (1 4) (2 3) qui ne font partie d'aucune base du groupe $\mathfrak{S}_4$.

D'autre part, quel que soit le nombre entier $n \geqslant 3$ ($n \geqslant 4$), le nombre total de bases du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) est un multiple de $n!/2$ ($n!/4$).

Nous disons que deux substitutions S, T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) sont *connexes* s'il n'existe aucun vrai sous-ensemble de l'ensemble $E = \{1 , 2, \ldots , n\}$ qui est transformé en lui-même aussi bien par la substitution S que par la substitution T. On voit immédiatement qu'une condition nécessaire (mais pas suffisante) 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 connexes.

Nous disons que deux substitutions connexes S, T du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) sont *imprimitives* si l'on peut décomposer l'ensemble $E = \{1 , 2 , \ldots , n\}$ en $m > 1$ sous-ensembles disjoints $E_1, E_2, \ldots, E_m (E_1 + E_2 + \cdots + E_m = E)$, comprenant chacun un même nombre $l > 1$ d'éléments, de façon que la substitution S aussi bien que la substitution T transforme chaque ensemble $E_i (1 \leqslant i \leqslant m)$ en un ensemble $E_j (1 \leqslant j \leqslant m)$. Nous disons que les deux substitutions S, T sont *primitives* dans le cas contraire.

D'après cette définition, si n est un nombre premier, deux substitutions connexes du groupe $\mathfrak{S}_n (\mathfrak{A}_n)$ sont toujours primitives.

Deux substitutions imprimitives engendrent, comme on voit sans

peine, un groupe imprimitif. Or, le groupe $\mathfrak{S}_n$ aussi bien que le groupe $\mathfrak{A}_n$ sont primitifs. Donc 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. Mais cette condition n'est, en général, pas suffisante. Ainsi les deux substitutions $S = (1\ 2\ 3\ 4\ 5)$, $T = (2\ 3\ 5\ 4)$ sont primitives, mais elles engendrent le groupe métacyclique et ne constituent une base ni de $\mathfrak{S}_5$ ni de $\mathfrak{A}_5$. De même, les deux substitutions $S = (1\ 2\ 3\ 4\ 5\ 6)$, $T = (1\ 2)\ (3\ 4)$ sont primitives, mais elles engendrent un groupe d'ordre 120 et ne constituent ni une base de $\mathfrak{S}_6$ ni une base de $\mathfrak{A}_6$.

Le but de la présente note est d'établir quelques critères généraux permettant de discerner des bases du groupe $\mathfrak{S}_n$ et du groupe $\mathfrak{A}_n$.

II°

Soient S, T deux substitutions imprimitives du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) et soient $E_1, E_2, \ldots, E_m$ ($E_1 + E_2 + \cdots + E_m = \{1, 2, \ldots, n\}$) $m > 1$ ensembles, disjoints deux à deux, comprenant chacun $l > 1$ d'éléments et qui sont transformés les uns dans les autres aussi bien par la substitution S que par la substitution T.

On voit immédiatement que tout cycle d'ordre $> l$ de chacune des substitutions S, T a pour ordre un multiple de l et ce cycle comprend tous les éléments d'un certain nombre d'ensembles E_i ($1 \leqslant i \leqslant m$) et ne comprend pas d'autres éléments. D'autre part, si un cycle de l'une des substitutions S, T est d'ordre $< l$, tous les éléments de ce cycle appartiennent nécessairement à un même ensemble E_i et tous les autres éléments de cet ensemble E_i font alors nécessairement partie de cycles d'ordre $< l$ de S ou de T, ne comprenant aucun élément d'un ensemble E_j ($j \neq i$). En outre, si $C = (a_1\, a_2 \ldots a_r)$ est un cycle d'ordre $r = r'l (r' > 1)$ de S ou de T, quel que soit le nombre entier i compris au sens large entre 1 et r', il existe un indice $j (1 \leqslant j \leqslant m)$, tel que $E_j = \{a_i, a_{i+r'}, a_{i+2r'}, \ldots, a_{i+(l-1)r'}\}$.

Les substitutions S, T étant connexes, quel que soit l'indice $i (1 \leqslant i \leqslant m)$, l'une au moins des substitutions S, T contient un cycle d'ordre $\geqslant 2l$, comprenant tous les éléments de l'ensemble E_i qui est transformé en un ensemble E_j ($j \neq i$, $1 \leqslant j \leqslant m$).

Il peut d'ailleurs arriver que tous les cycles de l'une des substitutions S, T soient d'ordre $< l$. Tous les cycles de la seconde de ces substitutions sont alors d'ordre $\geqslant 2l$.

Soit $S = (1\ 2\ 3\ 4)$. Les substitutions du groupe $\mathfrak{S}_4$ imprimitives

avec S sont les suivantes: $(1\ 2\ 3\ 4)$, $(1\ 4\ 3\ 2)$, $(1\ 2)\ (3\ 4)$, $(1\ 3)\ (2\ 4)$, $(1\ 4)\ (2\ 3)$, $(1\ 3)$, $(2\ 4)$, 1.

Deux substitutions primitives du groupe $\mathfrak{S}_4$ ($\mathfrak{A}_4$) constituent toujours une base de ce groupe.

Quel que soit le nombre entier composé $n \geqslant 4$ et quel que soit le diviseur m $(1 < m < n)$ de n, les deux substitutions $S = (1\ 2 \dots n)$, $T = (m+1\ 2\ 3 \dots m\ 1\ m+2 \dots n)$ ne sauraient constituer une base ni de $\mathfrak{S}_n$ ni de $\mathfrak{A}_n$. En effet, soit $n = l\,m$ $(l > 1)$. Posons $E_i = \{i, i+m, \dots, i+(l-1)\,m\}$, pour $i = 1, 2, \dots, m$. Les deux substitutions S et T transforment les ensembles E_i les uns dans les autres. Elles sont donc imprimitives, ce qui justifie notre remarque.

On démontre sans peine que quels que soient les nombres entiers $m > 1$ et $n > m$ ainsi que les m nombres $a_1, a_2, \dots, a_m$ de la suite $1, 2, \dots, n$ (dont a_1 est le plus petit), si le plus grand commun diviseur $D(n, m)$ des deux nombres n et m est $= 1$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \dots n)$, $T = (a_1 a_2 \dots a_m)$ soient imprimitives, c'est que $D(a_2 - a_1, a_3 - a_1, \dots, a_m - a_1, n) > 1$. Si $D(n, m) > 1$, la condition précédente est encore suffisante pour que les deux substitutions S, T soient imprimitives, mais elle n'est pas nécessaire, comme le prouve l'exemple suivant. Soit $S = (1\ 2\ 3\ 4\ 5\ 6)$, $T = (1\ 2\ 4\ 5)$. On a $m = 4$, $n = 6$, $D(2-1, 4-1, 5-1, 6) = 1$. Or, les deux substitutions S, T sont imprimitives puisqu'elles transforment chacun des ensembles du système $E_1 = \{1, 4\}$, $E_2 = \{2, 5\}$, $E_3 = \{3, 6\}$ en un ensemble du même système.

Donc, quels que soient les nombres entiers $m > 1$, $n > m$ ainsi que les m nombres $a_1, a_2, \dots, a_m$ de la suite $1, 2, \dots, n$, si $D(a_2 - a_1, a_3 - a_1, \dots, a_m - a_1, n) > 1$, les deux substitutions $S = (1\ 2 \dots n)$, $T = (a_1 a_2 \dots a_m)$ ne sauraient constituer une base du groupe $\mathfrak{S}_n$ ni du groupe $\mathfrak{A}_n$.

En particulier, quel que soit le nombre pair $n \geqslant 4$, si T est une substitution de $\mathfrak{S}_n$, telle que tous les éléments de chaque cycle de T sont simultanément des nombres pairs ou simultanément des nombres impairs, les deux substitutions T et $S = (1\ 2 \dots n)$ ne sauraient constituer une base de $\mathfrak{S}_n$.

Quel que soit le nombre entier composé $n = lm$ $(l > 1, m > 1)$, les deux substitutions $S = (1\ 2 \dots n)$, $T = (1\ 2 \dots m)\ (m+1 \dots 2m) \dots ((l-1)\,m+1 \dots lm)$ dont la première est circulaire et la seconde est régulière d'ordre m, ne sauraient constituer une base du groupe $\mathfrak{S}_n$ ni du groupe $\mathfrak{A}_n$.

En effet, ces deux substitutions sont imprimitives. Elles transforment

les ensembles $E_i = \{i\,,\, i+m\,,\, \ldots\,,\, i+(l-1)\,m\}$, $(i = 1\,,\, 2\,,\, \ldots\,,\, m)$, les uns dans les autres.

Quel que soit le nombre entier composé $n = lm = jk$ $(l > 1\,,\, m > 1\,,\, j > 1\,,\, k > 1\,,\, m \neq k)$, si $D(m\,,\, k) = r > 1$, les deux substitutions régulières connexes de degré n: $S = (1\ 2 \ldots m)\ (m+1 \ldots 2m) \ldots ((l-1)\,m+1 \ldots lm)$, $T = (1\ 2 \ldots k)\ (k+1 \ldots 2k) \ldots ((j-1)\,k+1 \ldots jk)$ ne sauraient constituer une base ni du groupe $\mathfrak{S}_n$ ni du groupe $\mathfrak{A}_n$.

En effet, soit $m = m'r\,,\, k = k'r$. On a $n = lm'r = jk'r$, donc $lm' = jk' = n'$. Posons $E_i = \{i\,,\, i+r\,,\, i+2r\,,\, \ldots\,,\, i+(n'-1)r\}$, $(i = 1\,,\, 2\,,\, \ldots\,,\, r)$. Chacune des substitutions $S\,,\, T$ transforme les ensembles E_i les uns dans les autres. Ces substitutions sont donc imprimitives.

Quels que soient les nombres entiers $r > 1\,,\, m_1\,,\, m_2\,,\, \ldots\,,\, m_r\,,\, a_1\,,\, a_2\,,\, \ldots\,,\, a_r$ $(1 = m_0 < m_1 < m_2 < \cdots < m_r = n,\ m_{i-1} \leqslant a_i \leqslant m_i\,,\, i = 1\,,\, 2\,,\, \ldots\,,\, r)$, si

$$*)\quad D(m_1\,,\, m_2 - m_1\,,\, \ldots\,,\, m_r - m_{r-1}) > 1\,,$$

les deux substitutions $S = (1\ 2 \ldots m_1)\ (m_1+1 \ldots m_2) \ldots (m_{r-1}+1 \ldots m_r)$, $T = (a_1\, a_2 \ldots a_r)$ ne sauraient constituer une base de $\mathfrak{S}_n$ ni de $\mathfrak{A}_n$. En effet, ont voit sans peine que les deux substitutions $S\,,\, T$ sont alors imprimitives.

Remarquons que la condition *) est suffisante pour que les deux substitutions $S\,,\, T$ soient imprimitives, mais elle n'est pas nécessaire, comme le montre l'exemple suivant:

Soit $S = (1\ 2)\ (3\ 4\ 5)\ (6\ 7)\ (8\ 9\ 10)$, $T = (1\ 3\ 6\ 8)$.

Ces deux substitions sont imprimitives. Elles transforment les uns dans les autres les ensembles $\{1\,,\, 6\}$, $\{2\,,\, 7\}$, $\{3\,,\, 8\}$, $\{4\,,\, 9\}$, $\{5\,,\, 10\}$. Or, $D(2\,,\, 3\,,\, 2\,,\, 3) = 1$.

Notations. Quels que soient les nombres entiers $r \geqslant 1\,,\, m_1\,,\, m_2\,,\, \ldots, m_r$ $(0 = m_0 < m_1 < m_2 < \cdots < m_r = n)$ et quels que soient les deux nombres a et b faisant partie d'un même cycle $C_i = (m_{i-1}+1 \ldots m_i)$ de la substitution $S = (1\ 2 \ldots m_1)\ (m_1+1 \ldots m_2) \ldots (m_{r-1}+1 \ldots m_r)$, nous appellerons *distance* entre a et b et nous désignerons par le symbole $\overline{ab}$ le plus petit nombre entier positif, tel que $a + \overline{ab} \equiv b$ (mod. $m_i - m_{i-1}$).

On démontre sans peine les propositions suivantes:

Propositions 1. Quels que soient le nombre entier $n \geqslant 3$ 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 qu'elles soient primitives, et,

pour qu'il en soit ainsi, il faut et il suffit que le plus grand commun diviseur $D(\overline{ab}, n)$ des deux nombres $\overline{ab}$ et n soit égal à 1.

Proposition 2. Quels que soient les nombres entiers $m \geqslant 1$, $n > m$ et $\geqslant 3$ ainsi que les deux nombres a, b de la suite $1, 2, \ldots, n$, dont l'un est $\leqslant m$ et l'autre est $> m$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b)$ constituent une base du groupe $\mathfrak{S}_n$, c'est que ces deux substitutions soient primitives, et pour cela il faut et il suffit que $D(m, n-m) = 1$.

Proposition 3. Quels que soient le nombre entier $n > 3$ 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 $\mathfrak{S}_n$ ($\mathfrak{A}_n$), si n est pair (impair), c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(\overline{ab}, \overline{ac}, n) = 1$.

Propositions 4. Quels que soient les nombres entiers $m \geqslant 1$, $n > m$ et > 3 ainsi que les trois nombres a, b, c de la suite $1, 2, \ldots, n$, 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 $\mathfrak{S}_n$ ($\mathfrak{A}_n$) si n est impair (pair), c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(m, n-m, d) = 1$, d désignant la *distance* entre les deux nombres du système a, b, c qui font partie d'un même cycle de S.

Proposition 5. Quels que soient les nombres entiers $l \geqslant 1$, $m > l$, $n > m$ et > 3 ainsi que les trois nombres entiers a, b, c dont un et un seul appartient à chacun des trois intervalles $< 1, l >$, $< l+1, m >$, $< m+1, n >$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots l)\ (l+1 \ldots m)\ (m+1 \ldots n)$, $T = (a\,b\,c)$ constituent une base du groupe $\mathfrak{S}_n$ ($\mathfrak{A}_n$) si n est pair (impair), c'est que ces deux substitutions soient primitives, et pour cela il faut et il suffit que $D(l, m-l, n-m) = 1$.

Proposition 6. Quels que soient le nombre entier $n \geqslant 7$ et les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(\overline{ab}, \overline{ac}, \overline{ad}, n) = 1$ et que l'on n'ait pas simultanément $\overline{ac} = \overline{bd} = \frac{n}{2}$.

Proposition 7. Quels que soient les nombres entiers $m \geqslant 2$, $n \geqslant m+2$ et $\geqslant 7$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont deux a, b sont $\leqslant m$ $(> m)$ et deux c, d sont $> m$ $(\leqslant m)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives et pour cela il faut et il suffit que $D(\overline{ab}, \overline{cd}, m, n-m) = 1$ et que l'on n'ait pas simultanément $\overline{ab} = \overline{cd}$, $\overline{ba} = \overline{dc}$.

Propositions 8. Quels que soient les nombres entiers $m \geqslant 2$, $n \geqslant m+2$ et $\geqslant 7$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont deux a, c sont $\leqslant m$ $(> m)$ et deux b, d sont $> m$ $(\leqslant m)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives et pour cela il faut et il suffit que $D(\overline{ac}, \overline{bd}, m, n-m) = 1$ et que l'on n'ait pas simultanément $\overline{ac} = \overline{ca}$, $\overline{bd} = \overline{db}$.

Proposition 9. Quels que soient les nombres entiers $m \geqslant 3$, $n > m$ et $\geqslant 7$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont trois a, b, c sont $\leqslant m$ $(> m)$ et le 4^{me} d est $> m$ $(\leqslant m)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives et pour cela il faut et il suffit que $D(\overline{ab}, \overline{ac}, m, n-m) = 1$.

Proposition 10. Quels que soient les nombres entiers $l \geqslant 2$, $m > l$, $n > m$ et $\geqslant 7$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont deux a, b sont $\leqslant l$, alors que $l+1 \leqslant c \leqslant m$, $m+1 \leqslant d \leqslant n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots l)\ (l+1 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(\overline{ab}, l, m-l, n-m) = 1$.

Proposition 11. Quels que soient les nombres entiers $l \geqslant 2$, $m > l$, $n > m$ et $\geqslant 7$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont deux a, c sont $\leqslant l$ alors que $l+1 \leqslant b \leqslant m$, $m+1 \leqslant d \leqslant n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots l)\ (l+1 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(\overline{ac}, l, m-l, n-m) = 1$ et que l'on n'ait pas simultanément $l = 2\,\overline{ac}$ et $m - l = n - m$.

Proposition 12. Quels que soient les nombres entiers k, l, m, n $(1 \leqslant k < l < m < n, n \geqslant 7)$ ainsi que les quatre nombres a, b, c, d de la suite $1, 2, \ldots, n$, dont un et un seul appartient à chacun des quatre intervalles $<1,k>$, $<k+1,l>$, $<l+1,m>$, $<m+1,n>$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots k)\ (k+1 \ldots l)\ (l+1 \ldots m)\ (m+1 \ldots n)$, $T = (a\ b\ c\ d)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives, et pour cela il faut et il suffit que $D(k, l-k, m-l, n-m) = 1$ et que l'on n'ait pas simultanément $k = m-l$, $l-k = n-m$.

Proposition 13. Quels que soient le nombre entier $n \geqslant 9$ ainsi que les cinq nombres a, b, c, d, e de la suite $1, 2, \ldots, n$, la condition nécessaire et suffisante pour que deux substitutions non identiques du groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$, dont l'une S est quelconque et la seconde $T = (a\ b\ c\ d\ e)$, constituent une base du groupe $\mathfrak{S}_n$ $(\mathfrak{A}_n)$, c'est qu'elles soient primitives.

III°

Nous avons établi ailleurs[1]) les lemmes et propositions suivants qui nous seront utiles dans la suite:

Lemme I. Quels que soient le nombre entier $n > 2$ ainsi que les k $(1 < k \leqslant n)$ nombres $a_1, a_2, \ldots, a_k$ (dont a_1 est le plus petit) de la suite $1, 2, \ldots, n$, si $D(a_2 - a_1, a_3 - a_1, \ldots, a_k - a_1, n) = 1$, en composant la substitution $S = (1\ 2 \ldots n)$ avec le groupe symétrique des substitutions des éléments $a_1, a_2, \ldots, a_k$, on obtient le groupe $\mathfrak{S}_n$.

Lemme II. Quels que soient le nombre entier $n \geqslant 4$ ainsi que les k $(2 < k \leqslant n)$ nombres $a_1, a_2, \ldots, a_k$ (dont a_1 est le plus petit) de la suite $1, 2, \ldots, n$, en composant la substitution $S = (1\ 2 \ldots n)$ avec le groupe alternant des substitutions des éléments $a_1, a_2, \ldots, a_k$, on obtient le groupe $\mathfrak{S}_n$, si n est pair, ou le groupe $\mathfrak{A}_n$, si n est impair.

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

Proposition II. Quels que soient les nombres entiers $m > 1$, $i (1 \leqslant i \leqslant m)$ et $n > i$, les deux substitutions $S = (1\ 2 \ldots m)$, $T = (i\ i+1 \ldots n)$, si elles sont distinctes, constituent une base du groupe

[1]) Commentarii Mathematici Helvetici, vol. 11, 1938—39, fasc. 1. Wiadomosci Matematyczne, t. 47, 1939.

$\mathfrak{S}_{\max.(m,n)}$, si l'un au moins des nombres m, $n-i+1$ est pair, ou une base du groupe $\mathfrak{A}_{\max.(m,n)}$, si ces deux nombres sont impairs, au trois exceptions suivantes près: (1 2 3 4), (3 4 5 6); (1 2 3 4), (2 3 4 5 6); (1 2 3 4 5), (3 4 5 6).

Proposition III. Quels que soient les nombres entiers $n > 3$, $k \geqslant 1$, i $(1 \leqslant i \leqslant n)$, $r (1 \leqslant r \leqslant n-2)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (i\ i+k\ i+2k \ldots i+rk)$, 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, $r+1$ est pair, ou du groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs, c'est que $D(k, n) = 1$.

Passons maintenant à la démonstration de trois nouvelles propositions concernant les bases du groupe symétrique et du groupe alternant.

Proposition 14. Quels que soient le nombre entier $n \geqslant 11$ et les six nombres a, b, c, d, e, f de la suite $1, 2, \ldots, n$, vérifiant les inégalités $1 \leqslant a < b < c < d < e < f \leqslant n$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (a\ b\ c\ d\ e\ f)$ constituent une base du groupe $\mathfrak{S}_n$, c'est qu'elles soient primitives.

Démonstration. Il suffit de prouver que la condition est suffisante. Supposons que les substitutions S, T sont primitives. On voit sans peine que la condition nécessaire et suffisante pour qu'il en soit ainsi, lorsque $D(n, 6) = 1$, c'est que *) $D(\overline{ab}, \overline{bc}, \overline{cd}, \overline{de}, \overline{ef}, n) = 1$ et, lorsque $D(n, 6) > 1$, c'est que l'on ait l'égalité *), mais que l'on n'ait pas simultanément les égalités $\overline{ab} = \overline{de}$, $\overline{bc} = \overline{ef}$, $\overline{cd} = \overline{fa}$, ni les égalités $\overline{ab} = \overline{cd} = \overline{ef}$, $\overline{bc} = \overline{de} = \overline{fa}$.

Posons $\overline{ab} = k_1$, $\overline{bc} = k_2$, $\overline{cd} = k_3$, $\overline{de} = k_4$, $\overline{ef} = k_5$, $\overline{fa} = k_6$.

On a $k_1 + k_2 + k_3 + k_4 + k_5 + k_6 = n$.

Les cas suivants sont à distinguer.

1. Parmi les nombres $k_1, k_2, k_3, k_4, k_5, k_6$ il y en a un qui est plus petit que les cinq autres. Soit, p. ex., k_1 ce nombre (le raisonnement est tous à fait analogue, quel que soit le plus petit des six nombres k_i, $i = 1, 2, 3, 4, 5, 6$).

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ b_1\ c_1\ d_1\ e_1\ f_1)$, où b_1, c_1, d_1, e_1, f_1 sont cinq nombres de la suite $1, 2, \ldots, n$, différents de a, b, c, d, e, f. Donc T et T_1 engendront, d'après la proposition I, le groupe symétrique des substitutions des éléments qu'elles permutent, groupe qui contient le groupe symétrique G des substitutions des éléments a, b, c, d, e, f

et, d'après *) et le lemme I, en composant S avec les substitutions de G, on obtient le groupe $\mathfrak{S}_n$. Donc S, T est bien une base de $\mathfrak{S}_n$ dans ce cas.

2. Parmi les nombres $k_1, k_2, k_3, k_4, k_5, k_6$ il y en a deux égaux entre eux et plus petits que les quatre autres. Il y a lieu de distinguer 3 cas:

a) $k_i = k_{i+1} \begin{cases} k_{i+2} \\ k_{i+3} \\ k_{i+4} \\ k_{i+5} \end{cases}$, b) $k_i = k_{i+2} \begin{cases} k_{i+1} \\ k_{i+3} \\ k_{i+4} \\ k_{i+5} \end{cases}$, c) $k_i = k_{i+3} \begin{cases} k_{i+1} \\ k_{i+2} \\ k_{i+4} \\ k_{i+5} \end{cases}$,

les indices > 6 devant être réduits mod. 6 et i pouvant prendre l'une des valeurs 1, 2, 3, 4, 5, 6. Le raisonnement étant tout à fait analogue pour les différentes valeurs de i, il suffit de traiter le cas où $i = 1$. Soit

$$\text{a)} \quad k_1 = k_2 \begin{cases} k_3 \\ k_4 \\ k_5 \\ k_6 \end{cases} .$$

On a $$T_1 = S^{k_1} T S^{-k_1} = (b\ c\ c_1\ d_1\ e_1\ f_1),$$

où c_1, d_1, e_1, f_1 sont quatre nombres de la suite $1, 2, \ldots, n$, différents de a, b, c, d, e, f. D'après la proposition II, T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. On en déduit sans peine que S, T est une base de $\mathfrak{S}_n$.

Soit b) $$k_1 = k_3 \begin{cases} k_2 \\ k_4 \\ k_5 \\ k_6 \end{cases} .$$

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ b_1\ d\ d_1\ e_1\ f_1)$, où b_1, d_1, e_1, f_1 sont quatre nombres de la suite $1, 2, \ldots, n, \neq a, b, c, d, e, f$. On vérifie sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$ aussi dans ce cas.

Soit c) $$k_1 = k_4 \begin{cases} k_2 \\ k_3 \\ k_5 \\ k_6 \end{cases} .$$

Dans ce cas, les substitutions T et $T_1 = S^{k_1} T S^{-k_1}$ sont imprimitives et n'engendrent pas le groupe symétrique des substitutions des éléments qu'elles permutent. Envisageons alors les nombres k_2, k_3, k_5, k_6.

Comme les substitutions S , T sont primitives, on ne saurait avoir $k_2 = k_3 = k_5 = k_6$. Trois cas sont possibles:

c_1) Parmi les nombres k_2 , k_3 , k_5 , k_6 il y en a un plus petit que les 3 autres.

c_2) Parmi les nombres k_2 , k_3 , k_5 , k_6 il y en a deux égaux entre eux et plus petits que les deux autres.

c_3) Parmi les nombres k_2 , k_3 , k_5 , k_6 il y en a trois égaux entre eux et plus petits que le 4^{me}.

Envisageons d'abord le cas c_1). Soit, p. ex., k_2 le plus petit des 4 nombres k_2 , k_3 , k_5 , k_6 .

Alors

$$T_1 = S^{k_2} T S^{-k_2} = (a_1 \; c \; c_1 \; d_1 \; e_1 \; f_1) ,$$

a_1 , c_1 , d_1 , e_1 , f_1 désignant cinq nombres de la suite 1 , 2 , ... , n , $\neq a$, b , c , d , e , f. D'après la proposition I, les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il en découle que S , T est une base de $\mathfrak{S}_n$.

On traite de façon tout à fait analogue les autres variantes du cas c_1.

Passons maintenant au cas c_2). Il y a lieu de distinguer trois variantes de ces cas.

c_{21}) $k_2 = k_3 \begin{cases} k_5 \\ k_6 \end{cases}$.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1 \; c \; d \; d_1 \; e_1 \; f_1)$, où a_1 , d_1 , e_1 , f_1 sont quatre nombres de la suite 1 , 2 , ... , n , $\neq a$, b , c , d , e , f. D'après la proposition II, T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il s'ensuit que S , T est une base de $\mathfrak{S}_n$.

Le cas où $k_5 = k_6 \begin{cases} k_2 \\ k_3 \end{cases}$ se traite de façon tout à fait analogue.

c_{22}) $k_2 = k_5 \begin{cases} k_3 \\ k_6 \end{cases}$. Comme les substitutions S , T sont primitives, on ne saurait avoir $k_3 = k_6$. Supposons, p. ex., que $k_3 < k_6$ (le raisonnement est tout à fait analogue si $k_3 > k_6$). Alors, si $k_3 \neq k_1 + k_2$, on a $T_1 = S^{k_3} T S^{-k_3} = (a_1 \; b_1 \; d \; d_1 \; e_1 \; f_1)$, a_1 , b_1 , d_1 , e_1 , f_1 désignant 5 nombres de la suite 1 , 2 , ... , n , $\neq a$, b , c , d , e , f. D'après la proposition I, les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent.

Si $k_3 = k_1 + k_2$, on a $T_1 = S^{k_3} T S^{-k_3} = (c \; b_1 \; d \; f \; e_1 \; f_1)$, b_1, e_1, f_1 désignant trois nombres de la suite 1 , 2 , ... , n , $\neq a$, b , c , d , e , f et

l'on vérifie sans peine que les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent.

Il s'ensuit, dans les deux cas, que S , T est une base de $\mathfrak{S}_n$.

On traite de façon tout à fait analogue les autres variantes du cas c_{22}.

$c_{23})$ $k_2 = k_6 \left\langle \begin{matrix} k_3 \\ k_5 \end{matrix} \right.$.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1\ c\ c_1\ d_1\ e_1\ a)$, où a_1 , c_1 , d_1 , e_1 désignent 4 nombres de la suite $1 , 2 , \ldots , n , \neq a , b , c , d , e , f$. On vérifie sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il en résulte que S , T est une base de $\mathfrak{S}_n$ aussi dans ce cas.

Passons enfin au cas $c_3)$. Supposons d'abord que $k_2 = k_3 = k_5 < k_6$.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1\ c\ d\ d_1\ f\ f_1)$, où a_1 , d_1 , f_1 sont trois nombres de la suite $1 , 2 , \ldots , n , \neq a , b , c , d , e , f$. On vérifie aisément que les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S , T est une base du groupe $\mathfrak{S}_n$.

Supposons maintenant que $k_2 = k_3 = k_6 < k_5$.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1\ c\ d\ d_1\ e_1\ a)$ et on vérifie sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il en résulte que S , T est une base de $\mathfrak{S}_n$. On traite de façon tout à fait analogue les autres variantes du cas $c_3)$.

3. Parmi les nombres $k_1 , k_2 , k_3 , k_4 , k_5 , k_6$ il y en a trois qui sont égaux entre eux et plus petits que les trois autres.

Trois cas sont alors à distinguer.

a) Les trois nombres égaux entre eux et plus petits que les trois autres nombres de la suite $k_1 , k_2 , k_3 , k_4 , k_5 , k_6$ sont consécutifs dans cette suite.

b) Deux de ces nombres sont consécutifs dans la suite $k_1 , k_2 , k_3 , k_4 , k_5 , k_6$.

c) Parmi les trois nombres de la suite $k_1 , k_2 , k_3 , k_4 , k_5 , k_6$ qui sont égaux entre eux et plus petits que les trois autres, il n'y a pas deux nombres consécutifs de la suite.

Envisageons d'abord le cas a). Il suffit de supposer, p. ex., que

$k_1 = k_2 = k_3 \left\langle \begin{matrix} k_4 \\ k_5 \\ k_6 \end{matrix} \right.$.

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ c\ d\ d_1\ e_1\ f_1)$, où d_1 , e_1 , f_1 sont trois nombres de la suite $1 , 2 , \ldots , n , \neq a , b , c , d , e , f$. D'après la propo-

sition II, les substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$. — Passons maintenant au cas b). Supposons d'abord que $k_1 = k_2 = k_4 \begin{cases} k_3 \\ k_5 \\ k_6 \end{cases}$.

On a alors $T_1 = S^{k_1} T S^{-k_1} = (b\ c\ c_1\ e\ e_1\ f_1)$, où c_1, e_1, f_1 sont trois nombres de la suite $1, 2, \ldots, n, \neq a, b, c, d, e, f$. On vérifie aisément que les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S, T est une bas de $\mathfrak{S}_n$.

Supposons maintenant que $k_1 = k_2 = k_5 \begin{cases} k_3 \\ k_4 \\ k_6 \end{cases}$.

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ c\ c_1\ d_1\ f\ f_1)$, c_1, d_1, f_1 désignant trois nombres de la suite $1, 2, \ldots, n, \neq a, b, c, d, e, f$. On voit sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il en résulte que S, T est une base de $\mathfrak{S}_n$.

On traite de façon tout à fait analogue les autres variantes du cas 3b.

Passons, enfin, au cas c). Il suffit de supposer, p. ex., que $k_1 = k_3 = k_5$. Envisageons alors les trois nombres k_2, k_4, k_6. Les substitutions S, T étant primitives, on ne saurait avoir $k_2 = k_4 = k_6$. Supposons que parmi les nombres k_2, k_4, k_6 il y en a un qui est plus petit que les deux autres. Soit, p. ex., k_2 ce nombre.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1\ c\ c_1\ d_1\ e_1\ f_1)$, où $a_1, c_1, d_1, e_1, f_1 \neq a, b, c, d, e, f$. D'après la proposition I, T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il s'ensuit que S, T est une base de $\mathfrak{S}_n$. Supposons maintenant que parmi les nombres k_2, k_4, k_6 il y en a deux égaux entre eux et plus petits que le 3$^{\text{me}}$. Soit, p. ex., $k_2 = k_4 < k_6$.

On a $T_1 = S^{k_2} T S^{-k_2} = (a_1\ c\ c_1\ e\ e_1\ f_1)$, les nombres a_1, c_1, e_1, f_1 étant $\neq a, b, c, d, e, f$ et l'on vérifie sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$. Les autres variantes du cas 3c se traitent de façon tout à fait analogue.

4. Parmi les nombres $k_1, k_2, k_3, k_4, k_5, k_6$ il y en a quatre égaux entre eux et plus petits que les deux autres. Deux cas sont à distinguer:

a) Les quatre nombres égaux de la suite $k_1, k_2, k_3, k_4, k_5, k_6$ qui sont inférieurs aux deux autres sont consécutifs dans cette suite.

b) Les quatre nombres de la suite $k_1, k_2, k_3, k_4, k_5, k_6$ qui sont

égaux entre eux et plus petits que les deux autres ne sont pas consécutifs.

Envisageons le cas a). Il suffit de supposer, p. ex., que $k_1 = k_2 = k_3 = k_4 \begin{cases} k_5 \\ k_6 \end{cases}$.

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ c\ d\ e\ e_1\ f_1)$, où e_1 et f_1 sont deux nombres de la suite $1, 2, \ldots, n, \neq a, b, c, d, e, f$. D'après la proposition II, les deux substitutions T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Il s'ensuit que S, T est une base de $\mathfrak{S}_n$.

Passons maintenant au cas b). Il suffit de supposer, p. ex., que $k_1 = k_2 = k_3 = k_5 \begin{cases} k_4 \\ k_6 \end{cases}$.

On a $T_1 = S^{k_1} T S^{-k_1} = (b\ c\ d\ d_1\ f\ f_1)$, où d_1 et f_1 sont deux nombres de la suite $1, 2, \ldots, n, \neq a, b, c, d, e, f$, et l'on vérifie sans peine que T et T_1 engendrent le groupe symétrique des substitutions des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$.

On traite de façon tout à fait analogue les autres variantes du cas 4.

5. Parmi les nombres $k_1, k_2, k_3, k_4, k_5, k_6$ il y en a 5 qui sont égaux entre eux et plus petits que le 6$^{\text{me}}$. Soit, p. ex., $k_1 = k_2 = k_3 = k_4 = k_5 = k < k_6$. Comme les deux substitutions S, T sont primitives, on a alors $D(k, n) = 1$ et, d'après la proposition III, les deux substitutions S, T engendrent donc le groupe $\mathfrak{S}_n$.

Comme les substitutions S, T sont primitives et que $n \geqslant 11$, on ne saurait avoir simultanément $k_1 = k_2 = k_3 = k_4 = k_5 = k_6$.

Notre proposition est ainsi entièrement établie.

Proposition 15. Quels que soient les nombres entiers $n \geqslant 7, r, k$ et m $(1 \leqslant r < r + k + 1 \leqslant m \leqslant n)$, la condition nécessaire et suffisante pour que les deux substitutions $S = (1\ 2 \ldots n)$, $T = (1\ 2 \ldots r\ r + k + 1\ r + k + 2 \ldots m)$ constituent une base du groupe $\mathfrak{S}_n$, si l'un au moins des deux nombres n, $m - k$ est pair, ou du groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs, c'est qu'elles soient primitives.

Demonstration. Il suffit de prouver que la condition est suffisante.

Supposons d'abord que la substitution T est du second ordre: $T = (1\ 2 + k)$. La proposition à démontrer résulte alors de la proposition 1 et la condition nécessaire et suffisante pour que les substitutions S, T soient primitives, c'est que $D(k + 1, n) = 1$.

Supposons maintenant que T est du 3$^{\text{me}}$ ordre. On a alors soit $T = (1\ 2\ 2 + k)$, soit $T = (1\ 2 + k\ 3 + k)$. Dans les deux cas, les

substitutions S, T sont primitives et, d'après la proposition 3, elles constituent une base du groupe $\mathfrak{S}_n$, si n est pair, ou du groupe $\mathfrak{A}_n$, si n est impair.

Soit $m - k = 4$. Trois cas sont alors possibles:

a) $T = (1\ 2\ 3\ 2+k)$, b) $T = (1\ 2+k\ 3+k\ 4+k)$,

c) $T = (1\ 2\ 2+k\ 3+k)$.

Dans les cas a) et b), les deux substitutions S et T sont toujours primitives. Elles engendrent donc, d'après la proposition 6, le groupe $\mathfrak{S}_n$.

Dans le cas c), la condition nécessaire et suffisante pour que les substitutions S, T soient primitives, c'est que $k+1 \neq \frac{n}{2}$ et lorsque cette condition est satisfaite, les deux substitutions S, T engendrent le groupe $\mathfrak{S}_n$, d'après la proposition 6.

On voit sans peine que si $m - k \geqslant 4$, une condition nécessaire et suffisante pour que les substitutions S, T soient primitives, c'est que l'on n'ait pas simultanément $2r = m - k$ et $k = n - m$. Supposons cette condition satisfaite.

Soit $m - k > 4$.

Si $m = n$, les substitutions S, T engendrent toujours, d'après la proposition II, le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. Supposons que $m < n$.

Si $r = 1$, on a $T = (1\ 2+k\ 3+k \ldots m)$, $T_1 = S\,T\,S^{-1} = (2\ 3+k \ldots m\ m+1)$. Les deux substitutions T et T_1 engendrent, d'après la proposition II, le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent et, d'après les lemmes I et II, en composant S avec les substitutions de ce groupe on obtient le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. S, T est donc bien une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$ dans ce cas.

On démontre de même que si $m = r + k + 1$, les substitutions S, T constituent une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Supposons maintenant que $m - k \geqslant 5$, $r \geqslant 2$, $k \geqslant 1$, $m - (k+r) \geqslant 2$, $n - m \geqslant 1$.

On voit sans peine que $T^{-1}S = R = (r\ r+1 \ldots r+k)\ (m\ m+1 \ldots n)$.

Si les deux nombres $k+1$ et $n - m + 1$ sont premiers entre eux, il existe deux nombres entiers s et t, tels que $R^s = (r\,r+1 \ldots r+k)$, $R^t = (m\ m+1 \ldots n)$ et chacune de ces substitutions engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, d'après la proposition II. Donc S, T est bien une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$ aussi dans ce cas.

Supposons que $D(k+1, n - m + 1) > 1$. Les cas suivants sont alors à distinguer:

I. Parmi les nombres r , k , $m - (r + k)$, $n - m$ il y en a un qui est le plus petit.

1. Soit r ce nombre.

On a $T_1 = S^r T S^{-r} = (r + 1\ r + 2 \ldots 2r\ 2r + k + 1\ 2r + k + 2 \ldots m + r)$. D'après nos hypothèses, $2r < r + k + 1 < 2r + k + 1 < < m < m + r \leqslant n$.

Les deux substitutions T et T_1 engendrent donc, d'après la proposition II, le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Il en résulte, d'après les lemmes I et II, que S , T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Le raisonnement est tout à fait analogue si $m - (r + k)$ est le plus petit des quatre nombres considérés ci-dessus.

2. Soit k le plus petit des 4 nombres r , k , $m - (r + k)$, $n - m$. Il faut alors distinguer les cas suivants:

a) $r = k + 1 = m - (r + k) \leqslant n - m$.

On a alors $T_1 = S^{k+1} T S^{-k-1} = (r + 1\ r + 2 \ldots r + k + 1\ 2r + k + 1 \ldots m + r)$ et les deux substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent, d'après la proposition I. On en déduit sans peine que S , T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

b) $r > k + 1 = m - (r + k)$.

On a alors $T = (1\ 2 \ldots r\ r + k + 1\ r + k + 2 \ldots r + 2k + 1)$.

Comme k est, par hypothèse, le plus petit des 4 nombres r , k , $m - (r + k)$, $n - m$, on a en plus $n - (r + 2k + 1) \geqslant k + 1$, d'où on déduit que $n - k > r + 2k + 1$.

Si $n - k = r + 2k + 2$, on a $R = (r\ r+1 \ldots r+k)\ (r+2k+1 \ldots n)$,

$R_1 = S^{-k} R S^{k} = (r - k \ldots r - 1\ r)\ (r + k + 1 \ldots n - k)$

$U = T R_1^{-1} = (1\ 2 \ldots r - k\ r + k + 1\ r + 2k + 2)$,

$R_2 = U^{-1} R U = (r\ r + 1 \ldots r+k)\ (r+2k+1\ r+k+1$
$r + 2k + 3 \ldots n)$,

$Q = R R_2^{-1} = (r + k + 1\ \ r + 2k + 2\ \ r + 2k + 3)$.

D'après la proposition II, cette dernière substitution engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. Donc S , T est bien, dans ce cas, une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Si $n - k > r + 2k + 2$, on a

$$Q = (r + 2k + 2\ \ r + 2k + 3)\ \ (n - k + 1\ \ r + k + 1) .$$

Si $n - k = r + 2k + 3$, on a

$$Q = (r + 2k + 2 \quad r + 2k + 3)\ (r + 2k + 4 \quad r + k + 1),$$
$$Q_1 = S^{-2} Q S^2 = (r + 2k \quad r + 2k + 1)\ (r + 2k + 2 \quad r + k - 1).$$
$$Q Q_1 = (r + k - 1 \quad r + 2k + 3 \quad r + 2k + 2)\ (r + 2k \quad r + 2k + 1)$$
$$(r + 2k + 4 \quad r + k + 1)$$
$$(Q Q_1)^2 = (r + k - 1 \quad r + 2k + 2 \quad r + 2k + 3)$$

et cette dernière substitution engendre avec S, d'après la proposition II, le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. Il en est donc de même de S et T.

Si $n - k > r + 2k + 3$, posons

$$Q_1 = S^{-1} Q S = (r + 2k + 1 \quad r + 2k + 2)\ (n - k \quad r + k).$$

On a $Q Q_1 = (r + 2k + 1 \quad r + 2k + 3 \quad r + 2k + 2)\ (n - k \quad r + k)$ $(n - k + 1 \quad r + k + 1)$.

$$(Q Q_1)^2 = (r + 2k + 1 \quad r + 2k + 2 \quad r + 2k + 3)$$

et cette substitution engendre avec S le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$, d'après la proposition II. Les substitutions S, T constituent donc bien une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$ dans le cas considéré.

c) $r = k + 1 < m - (r + k)$.

Ce cas se traite d'une façon tout à fait analogue au cas b).

d) Soit $r > k + 1$ et $m - (r + k) > k + 1$.

On a $R_1 = S^{k+1} R S^{-k-1} = (r + k + 1 \ldots r + 2k + 1)\ (m + k + 1 \ldots n\ 1\ 2 \ldots k + 1)$,

$$R R_1^{-1} = (r\, r + 1 \ldots r + k)\ (r + 2k + 1 \ldots r + k + 1)\ (1\ m\ m+1 \ldots m + k + 1 \quad k + 1 \quad k \ldots 2)$$
$$= C_1 C_2 C_3,$$

C_1 et C_2 désignant deux cycles d'ordre $k + 1$ et C_3 un cycle d'ordre $2k + 3$.

Comme les nombres $k + 1$ et $2k + 3$ sont premiers entre eux, il existe un nombre entier l, tel que $(R R_1^{-1})^l = C_3 = (1\ m\ m+1 \ldots m+k+1\ k + 1\ k \ldots 2)$. Or, $C_3^{-1} = (m\ 1\ 2 \ldots k + 1\ m + k + 1 \ldots m + 1)$ et cette dernière substitution engendre avec T le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent, d'après la proposition II. Il en résulte immédiatement que S, T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Le cas où $n - m$ est le plus petit des 4 nombres r, k, $n - (k + r)$, $n - m$ se traite de façon tout à fait analogue à celui où k est le plus petit de ces nombres.

II. Parmi les nombres de la suite r , k , $m-(r+k)$, $n-m$ il y en a deux qui sont égaux entre eux et plus petits que les deux autres. Cela peut être deux nombres consécutifs ou deux nombres non consécutifs de ladite suite. Soit a) $r = k < {}^{m-2r}_{n-m}$ (on traite de façon tout à fait analogue le cas où $m-(r+k) = n-m < {}^{r}_{k}$).

Envisageons la substitution $T_1 = S^r T S^{-r} = (r+1 \ldots 2r \ \ 3r+1 \ldots m+r)$. D'après nos hypothèses et d'après la proposition II, les substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Il s'ensuit que S, T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Soit b) $k = m-(r+k) < {}^{r}_{n-m}$ (on traite de façon analogue le cas $n-m = r < {}^{k}_{m-(r+k)}$). On a donc $r-k>0$ et $n-k>m$. Envisageons la substitution

$$T_1 = S^{-k} T S^k = (n-k+1 \ \ n-k+2 \ldots n \ \ 1 \ \ 2 \ldots r-k \ \ r+1 \ \ r+2 \ldots m-k).$$

D'après la proposition II, les substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Donc S , T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Soit c) $r = m-(r+k) < {}^{k}_{n-m}$. Comme les substitutions S , T sont primitives, $k \neq n-m$. Supposons, pour fixer les idées, que $k < n-m$. (Le cas où $k > n-m$ se traite d'une façon analogue).

On a $T = (1 \ \ 2 \ldots r \ \ r+k+1 \ldots 2r+k)$

$$T_1 = S^{k+1} \ T \ S^{-k-1} = (k+2 \ \ k+3 \ldots k+r+1 \ \ r+2k+2 \ldots 2r+2k+1).$$

D'après nos hypothèses, $n \geqslant 2r+2k+1$. Donc T et T_1 engendrent, d'après la proposition I, le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Il s'ensuit que S , T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

d) Soit $k = n-m < {}^{r}_{m-(k+r)}$.

Comme les substitutions S , T sont primitives, $r \neq m-(k+r)$. Supposons que $r < m-(k+r)$ (le raisonnement est tout à fait analogue si l'on suppose que $r > m-(k+r)$). Alors $m > 2r+k$.

On a $R = (r \ \ r+1 \ldots r+k) \ (m \ \ m+1 \ldots m+k)$.

$$R_1 = S^r \ R \ S^{-r} = (r-k \ \ r-k+1 \ldots r) \ \ (2r \ \ 2r+1 \ldots 2r+k).$$

$R_1 R = (r+1 \ \ r+2 \ldots r+k \ \ r-k \ \ r-k+1 \ldots r) \ \ (2r \ \ 2r+1 \ldots 2r+k) \ (m \ \ m+1 \ldots m+k)$. Nous obtenons une substitution

comprenant trois cycles dont le premier est d'ordre $2k+1$ et les deux autres sont d'ordre $k+1$ premier avec $2k+1$. Il existe donc un nombre entier t, tel que $(R_1 R)^t = Q = (r+1\ r+2 \dots r+k\ r-k\ r-k+1 \dots r)$. Les deux substitutions T et Q engendrent, d'après la proposition II, le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Il en résulte que S, T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

III. Parmi les nombres de la suite *) $r, k, m-(r+k), n-m$ il y en a trois égaux entre eux et inférieurs au 4me. Les trois nombres égaux sont alors forcément consécutifs dans la suite *). Deux cas sont alors à distinguer.

a) $r = k = m-(k+r) < n-m$. Donc $n-m \geqslant r+1$.

On a $T = (1\ 2 \dots r\ 2r+1\ 2r+2 \dots 3r)$.

$T_1 = S^{r+1} T S^{-r-1} = (r+2\ \ r+3 \dots 2r+1\ \ 3r+2 \dots 4r+1)$.

D'après nos hypothèses, $n \geqslant 4r+1$. Il s'ensuit, d'après la proposition I, que les deux substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Le cas où $m-(k+r) = n-m = r$ se traite d'une façon tout à fait analogue.

b) Soit $k = m-(k+r) = n-m < r$.

On a $T = (1\ 2 \dots r\ r+k+1 \dots r+2k)$,

$T_1 = S^k T S^{-k} = (1+k\ 2+k \dots r+k\ r+2k+1 \dots r+3k)$.

D'après la proposition II, les substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des éléments qu'elles permutent. Donc S, T est une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$.

Le cas où $n-m = r = k < m-(r+k)$ se traite d'une façon tout à fait analogue.

Comme les substitutions S et T sont primitives, on ne saurait avoir simultanément $r = k = m-(r+k) = n-m$.

La proposition 15 est donc établie.

Remarque. La proposition 15 est encore vrai pour $n < 7$, aux deux exceptions suivantes près: $S = (1\ 2\ 3\ 4\ 5\ 6)$, $T = (1\ 3\ 4\ 5)$;

$S = (1\ 2\ 3\ 4\ 5\ 6)$, $T = (1\ 2\ 3\ 5)$. Les substitutions de chacun de ces couples sont primitives. Toutefois, elles ne constituent pas une base du groupe $\mathfrak{S}_6$.

Proposition 16. Quels que soient les nombres entiers positifs a_1, a_2, a_3, ..., a_r ($r > 1$), il existe un nombre entier n suffisamment grand et tel que les deux substitutions $S = (a_1\ a_2 \dots a_r)$, $T = (1\ 2 \dots n)$ engendrent le groupe $\mathfrak{S}_n$, si l'un au moins des nombres r, n est pair, ou le groupe $\mathfrak{A}_n$, si ces deux nombres sont impairs.

Démonstration. On peut toujours choisir les notations de façon que a_1 soit le plus petit nombre de la suite $a_1, a_2, \dots, a_r$. Soit a_i ($2 \leqslant i \leqslant r$) le plus grand nombre de cette suite et soit $a_i - a_1 = d$, $D(a_2 - a_1, a_3 - a_1, \dots, a_r - a_1) = k$. Soit n le plus petit nombre entier $> 2d$ et premier avec k. On a $T_1 = T^d S T^{-d} = (a_i\ b_2\ b_3 \dots b_r)$, $b_2, b_3, \dots, b_r$ désignant r nombres de la suite $1, 2, \dots, n$ dont aucun n'appartient au système $a_1, a_2, \dots, a_r$. D'après la proposition I, les deux substitutions T et T_1 engendrent le groupe symétrique ou le groupe alternant des substitutions des éléments qu'elles permutent, groupe qui contient le groupe symétrique ou le groupe alternant des substitutions des éléments $a_1, a_2, \dots, a_r$. Et comme $D(k, n) = 1$, il résulte des lemmes I et II qu'en composant T avec les substitutions de ce dernier groupe, on obtient le groupe $\mathfrak{S}_n$ ou le groupe $\mathfrak{A}_n$. Donc S, T est bien une base de $\mathfrak{S}_n$ ou de $\mathfrak{A}_n$, c. q. f. d.

(Reçu le 15 juillet 1939.)