Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 21 (1948)

Artikel: Note sur les bases du groupe symétrique.
Autor: Piccard, Sophie
DOI: https://doi.org/10.5169/seals-18602

Note sur les bases du groupe symétrique

Par Sophie Piccard, Neuchâtel

Remarque 1. Soit n un entier ≥ 3 et soit $\mathfrak{S}_n$ le groupe symétrique d'ordre $n!$ dont les substitutions portent sur les éléments $1, 2, \ldots, n$.

Il existe, comme on sait, des couples de substitutions de $\mathfrak{S}_n$ — appelés bases de $\mathfrak{S}_n$ — qui engendrent le groupe $\mathfrak{S}_n$ tout entier par composition finie.

Soit A, B une base de $\mathfrak{S}_n$ et soit n l'ordre de A. Alors, quels que soient les entiers i et j, compris au sens large entre 1 et n, les deux substitutions A et A^iBA^j forment également une base de $\mathfrak{S}_n$, puisque A et B s'en déduisent aussitôt par composition finie et que A, B est une base de $\mathfrak{S}_n$.

Proposition 1. Quel que soit l'entier $n \geq 4$, quelle que soit la substitution circulaire A du groupe $\mathfrak{S}_n$ et quelle que soit la substitution B de $\mathfrak{S}_n$ qui forme avec A une base de $\mathfrak{S}_n$, les n^2 substitutions A^iBA^j $(i, j = 1, 2, \ldots, n)$ sont distinctes.

Démonstration. Pour des raisons de symétrie, il suffit de traiter le cas où $A = (1\ 2\ \ldots\ n)$. Soit B une substitution de $\mathfrak{S}_n$ qui forme avec A une base de $\mathfrak{S}_n$ et supposons, contrairement à ce qu'il s'agit de démontrer, qu'il existe quatre entiers i', j', i'', j'', compris au sens large entre 1 et n, vérifiant l'une au moins des inégalités ↑) $i' \neq i''$, $j' \neq j''$ et tels que 1) $A^{i'}BA^{j'} = A^{i''}BA^{j''}$.

De 1) on déduit 2) $B = A^{i'-i''}BA^{j'-j''}$.

Et comme on a l'une au moins des inégalités ↑), l'un au moins des nombres $i' - i''$, $j' - j''$ n'est pas congru à zéro modulo n.

Soit

$$i' - i'' \equiv i \pmod{n}, \qquad 1 \leqslant i \leqslant n\ ,$$

$$j' - j'' \equiv j \pmod{n}, \qquad 1 \leqslant j \leqslant n\ .$$

On a donc 3) $B = A^iBA^j$.

D'après la remarque précédente, l'un au moins des nombres i, j est $< n$. Montrons que les deux nombres i et j sont $< n$. En effet, supposons, par exemple, que $i = n$, donc $j < n$. Alors de 3) il résulte que $A^j = 1$,

ce qui est impossible, puisque la substitution A est circulaire d'ordre n. On voit de même qu'on ne saurait avoir $j=n$. Donc $1 \leq i < n$, $1 \leq j < n$. Montrons que $D(n, i) = D(n, j)$ [1].

En effet, soit

$$4) \quad D(n, i) = l \ , \quad n = n'l \ , \quad i = i'l \ ,$$

$$5) \quad D(n, j) = l' \ , \quad n = n''l' \ , \quad j = j'l' \ .$$

De 3) on déduit $B = A^{ki} B A^{kj}$, quel que soit l'entier $k \geqslant 1$. En particulier

$$\dagger) \quad A^{n'i} B A^{n'j} = B, A^{n''i} B A^{n''j} = B \ ,$$

et comme $n'i = i'n'l \equiv 0 \pmod{n}$, d'après 4), et

$$n''j = j'n''l' \equiv 0 \pmod{n} \ ,$$

d'après 5), il résulte de $\dagger$) que

$$6) \quad A^{n'j} = 1 = A^{n''i} \ .$$

Et comme A est circulaire d'ordre n, il résulte de 6) que

$$7) \quad n'j \equiv 0 \pmod{n} \quad \text{et} \quad n''i \equiv 0 \pmod{n} \ .$$

Or, comme $n = n'l$ et que $n = n''l'$ (voir 4) et 5)), les congruences 7) impliquent que j est un multiple de l et que i est un multiple de l'. Soit l'' le plus petit commun multiple de l et de l'. Comme chacun des deux nombres l et l' est un diviseur de n, de i et de j, on doit avoir

$$8) \quad D(n, i) \geqslant l''$$

et

$$9) \quad D(n, j) \geqslant l'' \ .$$

Mais de 4), 5), 8) et 9) il résulte que $l = l' = l''$.

Soit

$$B = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \ ,$$

où $b_1 b_2 \dots b_n$ est une permutation des nombres $1, 2, \dots, n$.

---

[1]) u et v étant deux entiers, $D(u,v)$ désigne leur plus grand commun diviseur.

Soit h un entier quelconque compris au sens large entre 1 et n. B transforme h en b_h. D'autre part, A^j transforme h en $h+j$ [2]), B transforme $h+j$ en b_{h+j} et A^i transforme b_{h+j} en $b_{h+j}+i$ [2]). Donc A^iBA^j transforme h en $b_{h+j}+i$ et, d'après l'égalité 3), on a

$$10) \quad b_{h+j} \equiv b_h - i \pmod{n} ,$$

quel que soit $h = 1, 2, \ldots, n$.

Deux cas sont maintenant à distinguer :

I) $D(n, i) = D(n, j) = 1$.

Alors chacune des deux suites de nombres

$$11) \quad 1 , 1+j , 1+2j , \ldots , 1+(n-1)j$$

et

$$12) \quad b_1, b_1 - i, b_1 - 2i , \ldots , b_1 - (n-1)i ,$$

réduits mod n, comprend tous les nombres de la suite $1, 2, \ldots, n$. Dans ce cas

$$b_{1+hj} \equiv b_1 - hi \pmod{n}, \quad h = 1, 2, \ldots, n ,$$

et

$$B = \begin{pmatrix} 1 & 1+j & \ldots & 1+(n-1)j \\ b_1 & b_1 - i & \ldots & b_1 - (n-1)i \end{pmatrix} ,$$

où b_1 est un nombre de la suite $1, 2, \ldots, n$.

Soit v le nombre de la suite $1, 2, \ldots, n$, tel que $vj \equiv 1 \pmod{n}$ et soit $-vi \equiv k \pmod{n}$, $1 \leqslant k \leqslant n$.

Alors

$$13) \quad B = \begin{pmatrix} 1 & 2 & \ldots & n \\ b_1 & b_1 + k & \ldots & b_1 + (n-1)k \end{pmatrix} ,$$

tous les nombres $b_1 + hk$ $(h = 1, 2, \ldots, n-1)$ devant être réduits mod n, de façon à être compris au sens large entre 1 et n.

Soit r l'ordre de la substitution B.

Montrons qu'on a les relations

$$14) \quad B^hA = A^{k^h} B^h , \quad h = 1, 2, \ldots, r .$$

---

[2]) $h+j$ et $b_{h+j}+i$ doivent être réduits modulo n de façon à être compris au sens large entre 1 et n.

En effet, d'après 13), on a

$$B^2 = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 + (b_1 - 1)k & b_1 + (b_1 - 1)k + k^2 & \dots & b_1 + (b_1 - 1)k + (n-1)k^2 \end{pmatrix},$$

$$B^3 = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 + (b_1 - 1)(k + k^2) & b_1 + (b_1 - 1)(k + k^2) + k^3 & \dots & b_1 + (b_1 - 1)(k + k^2) + (n-1)k^3 \end{pmatrix},$$

. . . . . .

$$B^h = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) & b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) + k^h & \dots & b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) + (n-1)k^h \end{pmatrix}.$$

Comme $B^r = 1$, on doit avoir

$$(b_1 - 1)(1 + k + k^2 + \dots + k^{r-1}) \equiv 0 \pmod{n} \quad \text{et} \quad k^r \equiv 1 \pmod{n}.$$

Soit p un nombre quelconque de la suite $1, 2, \dots, n$.

B^h transforme p en $b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) + (p-1)k^h$ et $A^{k^h} B^h$ transforme p en $b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) + pk^h$. D'autre part, A transforme p en $p + 1$ et $B^h A$ transforme p en $b_1 + (b_1 - 1)(k + k^2 + \dots + k^{h-1}) + pk^h$.

On a donc bien les relations 14), quel que soit $h = 1, 2, \dots, r$. Mais alors le groupe (A, B) engendré par les deux substitutions A et B ne comprend que des substitutions de la forme $A^{h'} B^h$ ($h' = 1, 2, \dots, n$, $h = 1, 2, \dots, r$). Donc le groupe (A, B) est d'ordre $\leqslant nr$. Et comme $B \in \mathfrak{S}_n$, on a $r < (n-1)!$, quel que soit $n \geqslant 4$.

Donc l'ordre du groupe (A, B) est $< n!$

Il s'ensuit que si on a la relation 3), A et B ne sauraient constituer une base de $\mathfrak{S}_n$, contrairement à notre hypothèse sur ces deux éléments [3]).

II) Soit $D(n, i) = D(n, j) = q > 1$.

Montrons que dans ces conditions les substitutions A et B sont imprimitives.

En effet, soit $i = i'q$, $j = j'q$, $n = n'q$.

---

[3]) La condition que $n \geqslant 4$ est essentielle. En effet, si $n = 3$ et si $A = (123)$ et $B = (13)$, on a $ABA = B$. Or, $(A, B) = \mathfrak{S}_3$.

On a, d'après ce qui précède,

$$A = (1, 2, \ldots, n) \ , \quad B = \begin{pmatrix} 1 & 2 & \ldots & n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

et, d'après 3) et 10), $b_{h+h'j} \equiv b_h - h'i \pmod{n}$, $h = 1, 2, \ldots, q$, $h' = 1, 2, \ldots, n' - 1$.

Donc, comme $i = i'q$, quel que soit l'entier h $(1 \leqslant h \leqslant q)$, les nombres $b_h, b_{h+j}, \ldots, b_{h+(n'-1)j}$ sont congrus deux à deux modulo q et, comme $b_1, b_2, \ldots, b_n$ est une permutation des nombres $1, 2, \ldots, n$, il s'ensuit que si l'on appelle c_h l'entier compris au sens large entre 1 et q, tel que $b_h \equiv c_h \pmod{q}$, alors $c_1, c_2, \ldots, c_q$ est une permutation des nombres $1, 2, \ldots, q$.

Et comme $j = j'q$, quel que soit l'entier h vérifiant les inégalités $1 \leq h \leq q$, les nombres h, $h + j, \ldots, h + (n' - 1)j$ sont congrus deux à deux modulo q. On peut donc répartir les nombres $1, 2, \ldots, n$ en q sous-ensembles

$$C_h = \{h, h + q, h + 2q, \ldots, h + (n' - 1)q\}, \quad h = 1, 2, \ldots, q,$$

disjoints deux à deux, d'ordre n' chacun et tels que chacune des substitutions A, B transforme ces ensembles C_h les uns dans les autres. Notamment A transforme C_h en C_{h+1}, $h = 1, 2, \ldots, q - 1$ et C_q en C_1, alors que B transforme C_h en C_{c_h}, $h = 1, 2, \ldots, q$. Donc les substitutions A et B sont imprimitives et, par suite, elles entendrent un groupe imprimitif. Or le groupe $\mathfrak{S}_n$ est primitif et, par suite, $(A, B) \neq \mathfrak{S}_n$, ce qui est contraire à notre hypothèse que A, B est une base de $\mathfrak{S}_n$.

On voit donc bien que, si $n \geqslant 4$, si A est circulaire et si B est une substitution de $\mathfrak{S}_n$ qui forme avec A une base de $\mathfrak{S}_n$, les n^2 substitutions $A^i B A^j$ $(i, j = 1, 2, \ldots, n)$ sont bien distinctes, c. q. f. d.

Corollaire 1. Quel que soit l'entier $n \geqslant 4$ et quelle que soit la base A, B du groupe $\mathfrak{S}_n$, dont l'une des substitutions A est circulaire, les couples A, $A^i B A^j$ $(i, j = 1, 2, \ldots, n)$ constituent n^2 bases distinctes du groupe $\mathfrak{S}_n$.

Démonstration. Soit n entier $\geqslant 4$ et soit A, B une base du groupe $\mathfrak{S}_n$, telle que A est circulaire. D'après la proposition 1, les n^2 substitutions $A^i B A^j$ $(i, j = 1, 2, \ldots, n)$ sont distinctes deux à deux et, d'après la remarque 1, chacune d'elles forme avec A une base de $\mathfrak{S}_n$. Ces n^2 bases sont distinctes deux à deux.

Proposition 2. Quel que soit l'entier $n \geqslant 4$ et quelle que soit la substitution circulaire A du groupe $\mathfrak{S}_n$, le nombre total des bases du groupe $\mathfrak{S}_n$ dont l'une des substitutions est A est un multiple de n^2.

Démonstration. Soit $A = (a_1 a_2 \ldots a_n)$ une substitution circulaire quelconque du groupe $\mathfrak{S}_n$ ($n \geqslant 4$) et soit E l'ensemble des substitutions de $\mathfrak{S}_n$ qui forment avec A une base de $\mathfrak{S}_n$. L'ensemble E n'est jamais vide puisqu'il contient en tout cas la substitution $(a_1 a_2)$.

Soit B_1 un élément quelconque de l'ensemble E et soit E_1 l'ensemble des substitutions $A^i B_1 A^j$ $(i, j = 1, 2, \ldots, n)$. D'après la proposition 1, E_1 contient n^2 substitutions distinctes et, d'après le corollaire 1, les couples A, $A^i B_1 A^j$ constituent n^2 bases distinctes du groupe $\mathfrak{S}_n$. On a donc $E_1 \subseteq E$.

Soit maintenant h un entier $\geqslant 1$ et supposons que nous ayons déjà défini h éléments $B_1, B_2, \ldots, B_h$ de E et h sous-ensembles $E_1, E_2, \ldots, E_h$ de l'ensemble E, disjoints deux à deux et tels que E_1 se compose des éléments $A^i B_1 A^j$ $(i, j = 1, 2, \ldots, n)$, quel que soit $l = 1, 2, \ldots, h$. Si $\sum_{l=1}^{h} E_l = E$, le théorème est démontré. Sinon, soit B_{h+1} un élément quelconque de l'ensemble $E - \sum_{l=1}^{h} E_l$ et soit E_{h+1} l'ensemble des substitutions $A^i B_{h+1} A^j$ $(i, j = 1, 2, \ldots, n)$. D'après la proposition 1 et le corollaire 1 les couples A, $A^i B_{h+1} A^j$ constituent n^2 bases distinctes du groupe $\mathfrak{S}_n$. Montrons que les ensembles E_{h+1} et $\sum_{l=1}^{h} E_l$ ne sauraient avoir aucun élément commun. En effet, supposons le contraire. Il existerait alors quatre entiers i_1, j_1, i_2, j_2 compris au sens large entre 1 et n ainsi qu'un entier l $(1 \leqslant l \leqslant h)$, tels que $A^{i_1} B_l A^{j_1} = A^{i_2} B_{h+1} A^{j_2}$, d'où il résulterait que $B_{h+1} = A^{i_1 - i_2} B_l A^{j_1 - j_2}$, donc $B_{h+1} \in E_l$, contrairement à notre supposition que $B_{h+1} \in E - \sum_{l=1}^{h} E_l$.

On a donc bien $E_{h+1} \sum_{l=1}^{h} E_l = 0$. Cela étant quel que soit l'entier $h \geqslant 1$ et tel que $E - \sum_{l=1}^{h} E_l \neq 0$, il s'ensuit que l'ordre de E est bien un multiple de n^2, c. q. f. d.

Proposition 3. Quel que soit l'entier impair $n \geqslant 5$, le nombre total des bases de $\mathfrak{S}_n$, dont l'une des substitutions est circulaire, est un multiple de n^2.

Démonstration. Soit n un entier impair $\geqslant 5$. Alors, comme toute sub-

stitution circulaire du groupe $\mathfrak{S}_n$ est de classe paire, deux telles substitutions ne sauraient constituer une base du groupe $\mathfrak{S}_n$. Il y a en tout $(n-1)!$ substitutions circulaires du groupe $\mathfrak{S}_n$. Soit $A = (a_1 a_2 \ldots a_n)$ une quelconque de ces substitutions. D'après la proposition 2, le nombre total des bases de $\mathfrak{S}_n$ dont l'une des substitutions est A est un nombre de la forme kn^2, où k désigne un entier positif indépendant de A. Et comme deux substitutions circulaires différentes ne sauraient faire partie d'une même base de $\mathfrak{S}_n$, le nombre total des bases de $\mathfrak{S}_n$, dont l'une des substitutions est circulaire est égal à $kn^2(n-1)!$ Ce nombre est bien un multiple de n^2, c. q. f. d.

Remarque 2. Pour $n = 5$, on a $k = 2$ et, pour $n = 7$, on a $k = 51$.

Remarque 3. Le proposition 3 est en défaut pour le groupe $\mathfrak{S}_n$, si n est un entier pair $\geqslant 4$. Ainsi, pour $n = 4$, le nombre total des bases de $\mathfrak{S}_4$ dont l'une des substitutions est circulaire est 84 et ce nombre n'est pas un multiple de $n^2 = 16$.

Bases du groupe $\mathfrak{S}_7$, dont l'une des substitutions est circulaire.

Dans notre livre „Sur les bases du groupe symétrique" (Librairie Vuibert, Paris 1946) nous avons indiqué (p. 98—100) un système complet de bases indépendantes du groupe $\mathfrak{S}_n$ pour $n = 3, 4, 5$ et 6. [4])

Voici, pour $n = 7$, l'ensemble des substitutions du groupe $\mathfrak{S}_7$ qui forment avec la substitution circulaire $A = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ une base du groupe $\mathfrak{S}_7$.

1) $(a\ b\ c\ d\ e\ f)$

où a, b, c, d, e, f sont six nombres quelconques de la suite

†) 1, 2, 3, 4, 5, 6, 7

à l'exception des substitutions $(aa + 2a + 1a + 5a + 3a + 4)$ et $(aa + 4a + 3a + 5a + 1a + 2)$, où a est un nombre quelconque de la suite †) et où les nombres > 7 doivent être réduits mod 7.

Ces substitutions forment, avec A, 826 bases distinctes de $\mathfrak{S}_7$.

---

[4] Relevons les erreurs d'impression qui se sont glissées à la page 99.

Première colonne : la base IV, (152) (346) a été omise ;
ligne 26, lire (123) (45), (16) (24)
ligne 37, lire (123) (45), (134) (256)
ligne 38, lire (123) (45), (143) (265)

Seconde colonne : ligne 23, lire V, (14) (23) (56).

2) $(a\,b)\,(c\,d)\,(e\,f)$,

où a, b, c, d, e, f sont six nombres quelconques de la suite †), à l'exception des substitutions $(a\;a+1)\,(a+2\;\;a+6)\,(a+3\;\;a+5)$, où a est un nombre quelconque de la suite †). Les substitutions de ce type forment, avec A, 98 bases distinctes de $\mathfrak{S}_7$.

3) $(a\,b\,c\,d)$,

où a, b, c, d sont quatre nombres quelconques de la suite †). Ces substitutions sont au nombre de 210.

4) $(a\,b)$,

où a et b sont deux nombres quelconques de la suite †). Ces substitutions sont au nombre de 21.

5) $(a\,b)\,(c\,d\,e)$,

où a, b, c, d, e sont cinq nombres quelconques de la suite †). Ces substitutions sont au nombre de 420.

6) $(a\,b)\,(c\,d\,e\,f\,g)$,

où a, b, c, d, e, f, g est une permutation quelconque des nombres 1, 2, 3, 4, 5, 6, 7. Ces substitutions sont au nombre de 504.

7) $(a\,b\,c\,d)\,(e\,f\,g)$,

où a, b, c, d, e, f, g ont la même signification que ci-dessus. Ces substitutions sont au nombre de 420.

Le nombre total des bases du groupe $\mathfrak{S}_7$ dont l'une des substitutions est A est égal à $2499 = 51 \cdot 49$.

Le nombre total des bases du groupe $\mathfrak{S}_7$ dont l'une des substitutions est circulaire est égal à $1 \cdot 799 \cdot 280$.

(Reçu le 10 juin 1947.)